National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-36

# Guide to Selecting Information Technology Security Products

## Recommendations of the National Institute of Standards and Technology

Timothy Grance
Marc Stevens
Marissa Myers

**NIST Special Publication 800-36**

# Guide to Selecting Information Technology Security Products

*Recommendations of the National Institute of Standards and Technology*

**Timothy Grance, Marc Stevens, Marissa Myers**

**C O M P U T E R  S E C U R I T Y**

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

October 2003


**U.S. Department of Commerce**

Donald L. Evans, Secretary

**Technology Administration**

Phillip J. Bond, Under Secretary for Technology

**National Institute of Standards and Technology**

Arden L. Bement, Jr., Director

# Acknowledgements

The authors, Timothy Grance of NIST, and Marc Stevens and Marissa Myers of Booz Allen Hamilton, wish to express their thanks to the staff at NIST and at Booz Allen Hamilton who reviewed drafts of this document and provided valuable insights that contributed substantially to the technical content of this document. We also gratefully acknowledge and appreciate the many comments we received from readers of the public and private sectors, whose valuable insights improved the quality and usefulness of this document. The authors would like to specifically acknowledge some key organizations whose extensive feedback substantially contributed to the development of the document. These organizations include: National Archives and Records Administration, Environmental Protection Agency, Department of Treasury, Small Business Administration, Tennessee Valley Authority, and Corbett Technologies. The authors would also like to acknowledge Ron Ross, Marianne Swanson, Tim Polk, Vincent Hu, John Wack, Murugiah Souppaya, Ramaswamy Chandramouli, Wayne Jansen, Arnold Johnson, Gary Stoneburner, Curtis Barker, Annabelle Lee, Ron Tencati, James Dray, and Bill Burr of NIST, Alexis Feringa, Ed Giorgio, Clark Hayden, Miles Tracy, Mark McLarnon, and Skip Hirsh of Booz Allen Hamilton, and Shirley Radack and Gene Troy for their extensive review and comment and keen and insightful assistance throughout the development of the document. Finally, the authors would like to acknowledge Jamie Gillespie at the Australian Computer Emergency Response Team and the time spent developing the very extensive comments that contributed greatly to the improvement of the document.

## Executive Summary

The selection of IT security products is an integral part of the design, development and maintenance of an IT security infrastructure that ensures confidentiality, integrity, and availability of mission critical information. This guide, NIST Special Publication (SP) 800-36, *Guide to Selecting Information Technology (IT) Security Products*, first defines broad security product categories and specifies product types within those categories. It then provides a list of characteristics and pertinent questions an organization should ask when selecting a product from within these categories.

The selection of IT security products, and the implementation of the security program within which these products are used, follows the risk management process of identifying the most effective mix of management, operational, and technical controls. The specific blend of security controls an organization employs is tied to the mission of the organization and the role of the system within the organization as it supports that mission. Risk management is the process used to identify an effective mixture of controls. Once the necessary controls are identified, IT security products can then be identified to provide for these controls using the considerations and questions discussed in this document.

The guide seeks to assist in choosing IT security products that meet an organization's requirements. It should be used with other NIST publications to develop a comprehensive approach to managing, satisfying, and verifying an organization's IT security and information assurance requirements. Related publications include the following:

- NIST SP 800-30, Risk Management Guide for Information Technology Systems
- NIST SP 800-27, Engineering Principles for Information Technology Security: A Baseline for Achieving Security
- NIST SP 800-23, Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Test/Evaluated Products
- NIST SP 800-53, Recommended Security Controls for Federal Information Systems
- NIST SP 800-64, Security Considerations in the Information System Development Life Cycle.

Depending on the product category, other NIST SPs may be relevant:

- NIST SP 800-41, An Introduction to Firewalls and Firewall Policy
- NIST SP 800-32, Introduction to Public Key Technology and the Federal PKI Infrastructure
- NIST SP 800-31, Intrusion Detection Systems
- NIST SP 800-33, Underlying Technical Models for Information Technology Security.

The following IT security product categories are covered in this document, with a discussion of the types of products, product characteristics, and environment considerations for each category:

- Identification and Authentication
- Access Control
- Intrusion Detection
- Firewall
- Public Key Infrastructure
- Malicious Code Protection
- Vulnerability Scanners
- Forensics
- Media Sanitizing.

In addition to a specific discussion of these product categories, the document recommends the following general considerations when selecting IT security products:

- Organizational considerations should include identifying the user community; the relationship between the security product and organization's mission; the sensitivity of the data; the organization's security requirements, policies, and procedures; and operational issues such as daily operation, maintenance, and training.
- Product considerations should include total life-cycle costs (including acquisition and support), ease-of-use, scalability, and interoperability requirements; test requirements; known vulnerabilities; implementation requirements for relevant patches; requirements and methods for reviewing product specifications against existing and planned organizational programs, policies, procedures, and standards; security critical dependencies with other products; and interactions with the existing infrastructure.
- Vendor considerations should include whether the selection of a particular product will limit future security choices; vendor experience with the product; and vendor history in responding to security flaws in its products.

# TABLE OF CONTENTS

# 1. Introduction

## 1.1 Authority

The National Institute of Standards and Technology (NIST) developed this document in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided A-130, Appendix III.

This guideline has been prepared for use by federal agencies. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright though attribution is desired.

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official.

## 1.2 Purpose and Limitations

A secure information infrastructure ensures confidentiality, integrity, and availability of mission critical information. Information technology (IT) security products are an integral component in the design, development, and maintenance of this secure infrastructure. It is important that IT security products operate as they were intended to provide a foundation for this secure infrastructure.

Objective grounds for confidence that security products work as intended are the basis for the concept of security assurance. Varying degrees of product assurance are supported through methods such as conformance testing, security evaluation, and trusted development methodologies. Assurance is not, however, a guarantee that the products work as intended in an operational (i.e. installed) environment. National Institute of Standards and Technology (NIST) Special Publication 800-23, *Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*, provides guidance to organizations that process sensitive information for the acquisition and use of security-related IT products.

This guide builds upon Special Publication 800-23 by describing the characteristics of several categories of IT security products. It also provides a set of questions that should be considered when procuring these products. This guide does not provide an exhaustive list of all IT security product categories as the commercial marketplace for IT security products is constantly changing. However, the questions provided in this guide can easily be modified for an organization's particular needs as the requirements and product environments evolve.

This guide should also be used in conjunction with Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, in developing a comprehensive set of security controls necessary for an organization to protect and secure its infrastructure.

Many IT security products are readily available for purchase in the commercial market. This guide will assist the reader in choosing IT security products that meet their organization's requirements.

This guide seeks to help organizations make informed decisions when selecting IT security products. The categories of products listed here include operational controls such as intrusion detection and technical controls such as firewalls. This guide should be used with other NIST publications to develop a comprehensive approach to the management of an organization's IT security and requirements. The guide first defines broad security product categories and then specifies product types within those categories. This guide explains and provides a list of characteristics and pertinent questions an organization should ask during the selection process.

## 1.3 Scope

This guide covers the selection of IT security products to be used as operational or technical security controls. It should be used after a risk assessment has been performed and the need for security controls established. This guide does not discuss how an organization should develop its overall IT security program or the optimal set of products that should be implemented. This guide covers many IT security product categories, but it is not exhaustive in its coverage. For instance, the issue of obsolescence is not addressed. Issues concerning one IT security product category may also be applicable to other product categories not described in this document. While covering broad IT security product categories, this guide does not attempt to be exhaustive in either coverage or depth of the many and varied products in the market place.

For information on the overall system security requirements analysis process and methods for incorporating security into IT procurements, see NIST Special Publication 800-64, *Security Considerations in the Information System Development Life Cycle*. For information on performing a risk assessment, see NIST Special Publication 800-30. For information on IT security engineering principles and concepts for an IT system, see NIST Special Publication 800-27, *Engineering Principles for Information Technology Security: A Baseline for Achieving Security* and NIST SP 800-33, *Underlying Technical Models for Information Technology Security*. For information regarding the acquisition of IT security services, see NIST SP800-35, *Guide to IT Security Services*. Finally, various security controls are described in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*.

## 1.4 Audience

This guide is written to help an organization during the various stages of the IT security product life cycle. It can be used as a tool by—

- IT Security Officers in gathering the necessary information for the IT risk assessment and building the business case for the procurement of IT security products
- Chief Information Officers (CIO) and Chief Technology Officers (CTO) in establishing product procurement policy and ensuring that security has been appropriately considered in the selection process
- IT directors, program managers, and system owners in understanding the types of available security products, what they should consider when making a selection decision, and what factors they should use for evaluating a security product.

## 1.5 Document Structure

This document is organized into five sections:

- Section 1 provides an introduction and describes the people who may benefit from security product guidance.
- Section 2 describes the roles and responsibilities of officials involved in the selection of IT security products.
- Section 3 provides an overview of security controls, outlining the steps an organization should take before selecting security products.
- Section 4 describes general product selection considerations.
- Section 5 describes security products, specific characteristics that should be considered when selecting a product, and associated environmental questions specific to a particular security product.

# 2. Roles and Responsibilities

Product selection involves numerous people throughout an organization. Each person involved in the process, whether on an individual or group level, should understand the importance of security in the organization's information infrastructure. Each organization may involve several subordinate organizations during the IT product selection process. The following roles are listed as a guide. Depending on the organization's needs, a person may be assigned one of the roles listed below or a combination of roles relevant to IT security needs. In some small organizations, a single individual may hold multiple roles.

## 2.1 IT Security Program Manager

The IT Security Program Manager is responsible for developing enterprise standards for IT security. This individual plays a leading role in introducing an appropriate, structured methodology to help identify, evaluate, and minimize IT security risks to the organization. IT security program managers coordinate and perform system risk analyses, analyze risk mitigation alternatives, and build the business case for the acquisition of appropriate security solutions that help ensure mission accomplishment in the face of real-world threats. They also support senior management in ensuring that security management activities are conducted as required to meet the organization's needs.

## 2.2 Chief Information Officer

The CIO is responsible for the organization's IT planning, budgeting, investment, performance and acquisition. As such, the CIO provides advice and assistance to senior organization personnel in acquiring the most efficient and effective security product to fit the IT security architecture.

## 2.3 IT Investment Board (or equivalent)

The IT investment board (or its equivalent) is responsible for managing the capital planning and investment control process defined by the Clinger-Cohen Act of 1996 (section 5). This board can set the investment criteria for security product selection in a qualitative and quantitative environment. The board can review benefits and risks for procuring a particular product and can be involved in examining alternative approaches.

## 2.4 Program Manager (owner of data) / Acquisition Initiator

The program manager represents programmatic interests during the security product acquisition process. Program managers play an essential role in security product selection because of their involvement in strategic planning initiatives and are intimately aware of functional system requirements.

## 2.5 Acquisition Team

The acquisition team is normally composed of representatives from program, technical, and contracting areas of the organization. It provides a balanced perspective of cost and schedule considerations. Further, the team ensures that security performance and investment objectives have been created and met successfully. Long- and short-term security needs must be considered during the security product selection. Information technology and information resource management personnel provide technical expertise to program management and contracting

officers involved in security product selection. They ensure that performance and engineering measures are met.

## 2.6 Contracting Officer[1]

The contracting officer is the person with the authority to enter into, administer, and/or terminate contracts and make related determinations and findings.

## 2.7 Contracting Officer's Technical Representative

The Contracting Officer's Technical Representative (COTR) is a qualified Government employee appointed by the Contracting Officer to act as their technical representative in managing the technical aspects of a particular contract.

## 2.8 IT System Security Officer

The IT System Security Officer is responsible for ensuring the security of an information system throughout its life cycle.

## 2.9 Other Participants

The list of roles in an IT acquisition can grow with the complexity involved in acquiring and managing IT systems. It is vital that all members of the acquisition team work together to ensure that a successful acquisition is achieved. Since the system certifier and accreditor must make critical decisions throughout the acquisition process, they could be included early in the acquisition process. System users may assist in the acquisition by helping the program manager to determine the need, refine the requirements, and inspect and accept the delivered system. Participants may also include personnel who represent information technology, configuration management, design/engineering, and facilities groups.

[1] Federal Acquisition Regulation Section 2.101

## 3. Selecting Proper Security Controls

A security program, whether at the organization or system level, should include an appropriate mixture of security controls: management, operational, and technical as described in NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*. A minimum set of system level controls may be found in the (draft) NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*. Management controls are techniques that are normally addressed by management in the organization's IT security program — focusing on managing the IT security program and risk. Operational controls are those controls that are operated by people, as opposed to a technology or to systems. Operational controls often rely on technical expertise, management controls, and technical controls. Technical controls emphasize the security controls that the computer system executes. These controls should be consistent with the operational context and management controls.

Reliance on technical controls alone will be insufficient without complementary management and operational controls. For example, an organization can install a robust firewall; however, if it allows unrestricted dialup access directly to the network, the organization will have significant vulnerabilities.

The number and type of appropriate security controls and their corresponding IT security products may vary throughout a particular system's development and procurement life cycles. The relative maturity of an organization's security architecture may influence the types of appropriate security controls. The blend of security controls is tied to the mission of the organization and the role of the system within the organization as it supports that mission.

Risk management is the process used to identify an effective mix of management, operational, and technical security controls to mitigate risk to a level acceptable to the responsible senior official. Although it may be tempting to simply pick a product off the shelf, using a risk management process to choose the most effective blend of controls enhances an organization's security posture. A risk management process, as described in NIST Special Publication 800-30, comprises three main phases: risk assessment, risk mitigation, and evaluation and assessment.

In the risk assessment phase, an organization analyzes identified threats and vulnerabilities in terms of likelihood of occurrence and expected loss, and determines the impact on its ability to fulfill its mission and/or business objectives. The outcome of this action will be a statement of the anticipated type and amount of damage that a threat could cause if a vulnerability were to be exploited successfully. This ensures that security requirements are prioritized and specific to the architecture.

In the risk mitigation phase, the organization identifies the types of controls that could be employed to reduce the level of risk to an acceptable level, as determined in the risk assessment. As mentioned above, these solutions may include management, operational, and/or technical controls. These controls may require the use of an IT security product. For instance, firewall and intrusion detection products are necessary elements of technical controls employed to limit the threats that can impact an organization's IT infrastructure. Once an organization has decided to implement a security technology, it should evaluate existing products in the context of its own security architecture to determine the best option.

Once the necessary controls are identified, specific IT security products can then be identified to provide for these controls. In addition, it is important to perform a cost-benefit analysis when selecting security products.[2] As part of the cost-benefit analysis, a life-cycle cost (LCC) estimate for the status quo and each alternative identified should be developed. In addition to LCC estimates, benefits associated with each alternative should be identified and, to the extent practicable, quantified in terms of dollar savings or cost avoidance.

Once all options are weighed in the cost-benefit analysis, the security product selection is made, and implementation of the product can follow.

[2] As with all aspects of risk management, analysis is performed at a level of rigor appropriate for the specific situation. For example, where the cost of a product is relatively low or the benefit is somewhat obvious a less rigorous analysis is likely to be appropriate. A typical example of such a situation is the use of an anti-virus product.

# 4. General Considerations

In addition to the topics discussed in the previous chapters, some other important factors should be considered by organizations when acquiring security products. Independent, third-party testing and evaluation of IT products gives consumers greater confidence that the security features in those products work as advertised by the vendor. Testing and evaluation also provides a way to demonstrate product compliance with organization security requirements and security standards. NIST Special Publication 800-23 provides guidance on security assurance and the use of tested/evaluated products, and should be consulted by organizations selecting security products for their IT systems and networks.

Two prominent security testing and evaluation programs are now in place to assess the security features and assurances of commercial off-the-shelf (COTS) products: (1) Common Criteria evaluation by the National Information Assurance Partnership[1] (NIAP) Common Criteria (CC) Evaluation and Validation Scheme (CCEVS) or a foreign evaluation scheme with the results recognized by CCEVS under the *Arrangement on the Mutual Recognition of Common Criteria Certificates in the Field of IT Security* (CCRA) and (2) NIST Cryptographic Module Validation Program[2] (CMVP). The NIAP CCEVS employs a network of private sector, accredited testing laboratories to independently evaluate commercial security products in a variety of key technology areas against a set of security requirements and specifications from the international standard, International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 15408, *Common Criteria for IT Security Evaluation*. The CMVP, also using independent, accredited, private-sector laboratories, focuses on security testing of cryptographic modules for conformance to Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, and related federal cryptographic algorithm standards. In both programs, a government body validates the results of the testing and evaluation processes to ensure that the security standards are being applied correctly and consistently.

In addition to gaining confidence from acquiring security products tested and evaluated under the NIAP CCEVS, a recognized foreign CC scheme, and NIST CMVP, consumers also benefit in another way. The evidence produced during the product testing and evaluation process (available in different forms depending on the program) can be used by systems integrators to build more secure systems and networks. System certifiers can also use this evidence to more effectively assess the security of an IT system in its operational environment in support of system accreditation.

As stated in NIST Special Publication 800-23, particular attention should be given to products that provide the needed security capabilities and that have been evaluated under either the CCEVS or CMVP program. The following sets of questions are product-independent and should be considered when forming a decision and selecting any product. These questions are organized into three categories: those that apply to the organization, those that apply to the product or its operation, and those that apply to the vendor. It should be noted, however, that these questions are neither exhaustive nor relevant in all circumstances. Depending on a person's role or perspective on the security product, a question may be more appropriately organized under another category. Organizations should use these questions as a guide and edit them as necessary for their unique circumstances. Furthermore, additional questions and considerations are needed

[1] See http://niap.nist.gov
[2] See http://csrc.nist.gov

to guide decisions that are consistent with the organization's architecture and a well-established business case.

### Organizational Questions

These questions are applicable to all information systems (for example, identification of all components, impact on system of emerging technologies, and use of appropriate contract language).

- Is the product necessary to adequately mitigate risk?
- Is the anticipated user community identified? How many and what type of users does the organization anticipate will use the security product?
- Is the relationship between this security product and the organization's mission performance understood and documented?
- Has the organization determined the sensitivity of the data to be protected?
- Are the organization security requirements supported by the security plan, policies and procedures?
- Have security requirements been identified and compared against product specifications?
- When selecting products, organizations need to consider the threat environment and the security functions needed to cost-effectively mitigate the risks to an acceptable level. Organizations should give consideration to acquisition and deployment of IT security products that have been evaluated and tested by independent accredited laboratories against appropriate security specifications and requirements. Examples of these specifications include protection profiles based on ISO/IEC 15408, the *Common Criteria for IT Security Evaluation*. However, agencies should consider their overall requirements and select products accordingly. In the case of cryptographic modules, when agencies have determined the need to protect information via cryptographic means, they may only select CMVP validated cryptographic modules. See http://csrc.nist.gov/cryptval/ for a validation list for cryptographic standards.
- Is communication required across a domain boundary (implies the need for a boundary controller; e.g., sub-system of firewall, intrusion detection system, and/or routers)?
- Is the security product consistent with physical security and other policy requirements?
- Has the impact on the enterprise operational environment where this product will operate been considered?
- Have security reviews included requirements for support, plug-in components, or middleware?

### Product Considerations

These questions are applicable to all information systems (for example, total life-cycle cost and acceptance testing).

- If the product has been evaluated under a CC scheme, validation test reports can be examined to avoid duplication of tests already performed as part of the independent evaluation process.

- Have known product vulnerabilities been addressed by reviewing the relevant vulnerabilities of a product? Known vulnerabilities for many products can be found using the NIST ICAT Vulnerability Search Engine (http://icat.nist.gov).[3]
- Have all relevant patches been tested and implemented?
- Have relevant existing CC protection profiles (PP) been reviewed (for example, http://niap.nist.gov/cc-scheme/PPRegistry.html and http://www.commoncriteria.org/protection_profiles/pp.html), to identify PPs that express security requirements applicable to the organization's needs in the anticipated threat environment? If existing protection profiles are not adequate, organizations should consider the usefulness of similar protection profiles as a starting point for examining products that might satisfy requirements applicable to the new environment.
- Have the lists of validated products (for example, http://niap.nist.gov/cc-scheme/ValidatedProducts.html) been reviewed? Products independently tested and validated under NIAP-CCEVS (or mutually recognized) provide some level of security assurance that the security functions of the product work as specified. In general, third party testing and evaluation can provide a significantly greater basis for customer confidence than is available from unevaluated products. Note, however, that purchasing an evaluated product simply because it is evaluated and without due consideration of applicable functional and assurance requirements and vendor reliability, may be neither useful nor cost effective. Organizations should consider their overall requirements and select the best products accordingly.
- Has the list of CMVP validated products been reviewed? Validated products are mandatory and binding on federal agencies where they have determined information must be protected via cryptographic means. This applies to all IT products irrespective of whether the product is a security product or whether the cryptographic module is embedded within another product (e.g. a database).
- Has the vendor's policy or stance on re-validation of products when new releases of the product are issued been considered?
- Have product specifications been reviewed with respect to existing and planned organizational programs, policies, procedures, and standards? Examples include an organization's:
  - Web policy
  - Public key infrastructure (PKI) program and policy
  - Smart card program
  - Network interconnection and approval policy.
- Does the product have any security critical dependencies on other products? For example, an operating system (OS) or cryptographic module?

[3] ICAT is a search engine for an industry standard set of known vulnerabilities (http://cve.mitre.org) containing links to vulnerability and patch information.

- Does interfacing the new product with the existing infrastructure introduce new vulnerabilities or interdependencies?
- What is the frequency of product failures and adequacy of corrective actions?

**Vendor Considerations**

These questions are applicable to all information system vendors (for example, long-term viability).

- Will the selection of a particular product limit the future choices of other IT security modifications and improvements? (Note: The change and pace of technology may make it difficult to estimate the impact to an organization's future security architecture.)
- Does the vendor have experience in producing high quality IT security products?
- What is the vendor's "track-record" in responding to security flaws in its products?
- How does the vendor handle software and hardware maintenance, end user support, and maintenance agreements?
- Does the vendor have an associated security or configuration guide for the product? Does the vendor use or make reference to NIST, consortia, or other consensus-based checklists, security configurations/settings or benchmarks.

# 5. IT Security Products

The following categories of security products represent common technological elements helpful in securing IT systems and supporting infrastructure. This list is not all-inclusive and will change over time. New products are introduced, and obsolete products are removed from the market constantly.

Each security product category discussion consists of four sections. The first is a general discussion of the security capability that this product category provides. The second describes the types of products that are available. Next, general product characteristics are provided. Finally, environmental questions are listed to help further refine the product requirements and assist in product selection.

Specific product vendors or products are not listed. These guidelines are vendor independent and not a review of specific products.

## 5.1 Identification and Authentication

NIST Special Publication 800-12 defines identification as the means by which a user provides a claimed identity to the system. Authentication is the means of establishing the validity of this claim. Authorization is the process of defining and maintaining the allowed actions. Identification and authentication establishes the basis for accountability and the combination of all three enables the enforcement of identity-based access control.

The user's identity can be authenticated using the following mechanisms:

- Requiring the user to provide something they have (e.g., token)
- Requiring the user to provide something they alone know (e.g., password)
- Sampling a personal characteristic (e.g., fingerprint).

The principal forms of authentication include static, dynamic, and multiple factor.

**Static**. Static authentication reuses a specific authenticator (e.g., static password). This type of authentication only provides protection against attacks in which an imposter cannot obtain the authenticator. The strength of the authentication process is highly dependent on the difficulty of guessing or decrypting the authenticator values and therefore how well they are protected in transit and while stored on the system.

**Dynamic.** Dynamic authentication uses cryptography or other techniques to create one per-session authenticator. A dynamic authenticator changes with each authentication session between the claimant and verifier.

**Multiple Factor.** Multiple-factor authentication requires two or more types of authentication techniques. Multiple factor authentication can include both static and dynamic authentication mechanisms. One example is the use of a password along with a smart card token.

Authorization mechanisms fall into four major categories:

**Local:** Local authorization is performed for each application and machine to which a user requires access. The mechanisms of the local operating system and applications are employed to setup and maintain the authorizations for that machine or application.

**Network:** Authorization is performed at a central, authorization server, providing access to a user's account from one or more workstations on the network. The key here is that the access is to a single user account. If the user requires multiple accounts, then each is a separate authorization and handled in like manner to multiple users.

**Single Sign-on:** Single sign-on employs a central authorization server to enable a user to authenticate one time in order to achieve access to multiple applications, machines, and domains operating with a variety of authentication mechanisms (for example, a Kerberos implementation within a heterogeneous Windows 2000 and Unix network). The central server contains identifier/authenticator pairs for each domain that the user needs to access and performs an authentication on behalf of the user for each resource that the user is authorized to access. The central server establishes and maintains, as individual actions, the authorizations at each application, machine, or domain that the user is allowed to access.

**Single Log-on:** Single log-on is similar to single sign-on with the exception that the central server authentication mechanism is the mechanism used by all the applications, machine, and domains with which the user needs to interact. Rather than store identifier/authenticator pairs for each verification, the one-time verification is accepted by all resources as the only verification needed. Additionally, the authorizations are maintained at the central server and the individual applications, machines, and domains query the central location to determine whether a specific access is authorized. Single log-on eliminates the need for authorization at each resource and for individual authentications to each resource.

### 5.1.1 Types of Products

Some examples of authentication products are provided below. These categories of authentication products are not mutually exclusive (e.g., some products may include one or more of the categories).

**Security Tokens.** Security tokens are used to allow access first to a computer and then to a network. Tokens come in various forms - for example, Personal Computer Memory Card International Association (PCMCIA) cards, flash memory, USB tokens, smart cards, and software.

- **PCMCIA Security Tokens**. These tokens offer a full suite of security services in portable format on a small card. PCMCIA cards can protect secret values adequately in most cases while still leaving room for additional physical tamper protection mechanisms. Disadvantages include a requirement for a PCMCIA card reader. Although common on laptop computers, PCMCIA card readers are not common in desktop computers. This imposes a significant added cost factor. The added expense of purchasing a card reader for every desktop workstation may be cost prohibitive especially in organizations with large numbers of desktop computers.

- **Smart Card Tokens**. Smart cards are replacing PCMCIA cards in many security token applications. Smart cards are credit-card size plastic cards with an embedded computer chip. The chip can be either a microprocessor with internal memory or a memory chip

with nonprogrammable logic. The chip connection is made by either direct physical contact or remotely via a contactless electromagnetic interface.

**Certificates**. The public key certificate associates a certificate holder's identity with his public key. (See Section 5.5, Public Key Infrastructure, for further details)

**Authentication Protocols.** These protocols are used to determine who is accessing a resource. Examples include the following:

- **RADIUS**. Using the Remote Authentication Dial-In User Service (RADIUS) protocol, a remote client can exchange authentication, access control, accounting, and device configuration information with a RADIUS server. The RADIUS server can authenticate a user or a device from its database or user I&A parameters.
- **TACACS+**. Terminal Access Controller Access Control System + (TACACS+) protocol enables a network resource to offload the user administration to a central server.

**Biometrics**. Biometrics are used for physical access control, electronic access control, and monitoring devices. An organization's choice of biometric control depends on the security level required, user acceptance, enrollment speed, and costs incurred.

Biometrics technology is used to identify and authenticate an individual based on personal characteristics. Examples of personal characteristics include fingerprints, face, retina, iris, speech, handwriting, hand geometry, and wrist veins.

Biometrics can also be combined with passwords, personal identification numbers (PIN), and cards to further increase accuracy and security.

### 5.1.2 Identification and Authentication Product Characteristics

Desired characteristics of effective identification and authentication products (including systems developed around key identification and authentication mechanisms) are:

- Capable of requiring users to identify themselves uniquely before being allowed to perform any actions on the system unless user anonymity or other factors dictate otherwise.
- Capable of internally maintaining the identity of all active users and as necessary be able to link defined security-relevant actions to specific users.
- Capable of supporting organization password policies, including length, complexity, and lifetime.
- Have advanced capabilities, such as antispoofing and allowing the use of tokens such as smart cards.
- Provide for efficient identification (ID) of users and password or token management.
- Have a secure I&A management capability that stores and transmits I&A data in encrypted form.
- Have an ability to log defined security events and sends alerts messages to the appropriate security administrators.

### 5.1.3 Environment Questions

#### *Smart Card Specific* [4]

#### Organizational Considerations

- How many individuals in the organization will use the product?
- How will the organization issue the cards?
- Will the organization use an automated database system to enter user-specific information onto the cards, or will manual processes be applied? Where will the database reside?
- Who will control the cards?
- Will readers be distributed to ensure that the implementation will be effective?
- Does the organization plan to use the card as the sole means of authentication?
- Does the organization have procedures in place to quickly deactivate lost or stolen cards?
- Are the cards interoperable among other authentication products and mechanisms across the organization?

#### Product Considerations[5]

- What major functions will the card be expected to perform?
- What kind of data will the card be used to store?
- What are the memory requirements for the card?

#### *Biometric Specific*

#### Organizational Considerations

- How many individuals does the organization expect to use the product and what is the distribution of biometric characteristics in the enrolled population?
- What areas does the organization plan to protect with the product—physical access, electronic access, or as a monitoring device?
- Is the organization more concerned with false positives (incorrectly admitting an unauthorized person) or false negatives (incorrectly denying access to an authorized person), and how much error is tolerable?

#### Product Considerations

- How well does the product automate enrollment, verification, and identification?

[4] These questions should be addressed by organizations that are considering deployment of storage and/or processor card-based technologies to support identification and authentication functions. Answers to these questions will help the organization to establish required technical characteristics, infrastructure requirements, organizational responsibilities and coordination requirements, and infrastructure and recurring cost parameters.

[5] NIST Interagency Report 6887-2003 Edition, Government Smart Card Interoperability Specification (GSC-IS), v2.1, July 2003 defines an architectural model for interoperable smart card service provider modules.

- Is the enrolled template stored locally on a card or in the reader, or is the enrolled template stored remotely in a central database?
- Are the communication paths between the offered template and enrolled template protected?
- Does either the enrolled template or threshold change with each successful verification?
- Does the system log accepted and failed attempts?
- Can end users enroll themselves?
- Does the application support remote enrollment?
- Does the application support remote access?
- Is the application interoperable with smart cards?
- Is the relation between Type I and Type II errors selectable and is there a ratio supported by the product that will meet both the security and operational requirements of the organization in the intended operational environment of the product?

## 5.2 Access Control

Access control ensures that only authorized access to resources occurs. Access control helps protect confidentiality, integrity, and availability and supports the principles of legitimate use, least privilege, and separation of duties. Access control simplifies the task of maintaining enterprise network security by reducing the number of paths that attackers might use to penetrate system or network defenses.

Access control systems[6] grant access to information system resources to authorized users, programs, processes, or other systems. Access control may be managed solely by the application, or it may use controls on files. The system may put classes of information into files with different access privileges. Controlling access can be based on any or a combination of the following:

- User identity
- Role memberships
- Group membership
- Other information known to the system.

By controlling who can use an application, database record, or file, an organization can help to protect that data. It is particularly important to control who is allowed to enable or disable the security features or to change user privileges.

Users need to ensure that secure applications sufficiently manage access to data that they maintain. Access control includes any or all of the following: knowing who is attempting access, mediating access according to some processing rules, and managing where or how data is sent.

[6] Access control systems are in many cases, not standalone systems, but capabilities of a larger system, like an operating system. This section addresses the characteristics and questions for access control systems, capabilities, and functions.

**Identity-based Access Control.** A security policy based on comparing the identity of the subject (user, group of users, role, process, or device) requesting access and the authorizations for this identity associated with the object (system resource) being accessed.

**Information Flow Control.** Information flow policies dictate whether information with a particular characteristic can move from one controlled entity (container or subject) to another. Information flow control is based on some fundamental characteristic of the information (not the container), and might not involve an identifiable subject.

### 5.2.1 Types of Products

**Access Control Lists**. Access control data can reside either in (a) the resource to be protected or (b) a central location based on a model. An example of a data structure used for resource-centric storage of access control information is the Access Control List (ACL). An example of a specification of access control information centrally based on a model is the role-based access control (RBAC) database.

ACLs in routers and other network devices can be used to implement the following forms of access enforcement:

*Traffic Filters.* Access controls can be enforced effectively at the data packet layer. A filter can block any packet that does not conform to security policy rules. Filters can be assigned to incoming or outgoing traffic. Filtering can be based on source and destination addresses, protocol types, and information from other fields within the packets unless the content is encrypted.

*Policy Filters.* Policy filters can be used to set up access control policies on routers. Policy filters, which operate to and from routing tables, can be used to specify the routers or networks from which updates will be accepted.

**Role-Based Access Control**. RBAC has emerged as a promising feature of many database management, security management and network operating system products. The essential advantage of RBAC products is that they allow system administrators to assign individual users into roles. The role identifies users as members of a specific group, based on their capabilities, work requirements, and responsibilities in the organization. Access rights, or security privileges, are then established for each role; a user may belong to multiple roles, which provide the appropriate level of access for their requirements. Thus, the RBAC structure empowers administrators with a tool to regulate which users are given access to certain data or resources, without having to explicitly authorize each user to each resource.

### 5.2.2 Access Control Product Characteristics

Desired characteristics of access control products are that they can:

- Support granularity of control (e.g., at the element and attribute level for XML documents)
- Allow simultaneous profile/rule assignment to a list of user accounts
- Define access privileges for each user
- Prevent unauthorized forwarding of sensitive information

- Provide for a central administration console for management and enforcement of security policies across distributed systems, if the product will be managed centrally
- Self-protect against outside attack
- Provide support for sophisticated rules checking
- Support content filtering (e.g., objectionable content, malicious code, viruses)
- Add cryptographic algorithms or cryptographic modes and add/modify filters
- Track any type of security related event through the log file
- Generate checksums to ensure the integrity of log files.

### 5.2.3 Environment Questions

#### Organizational Considerations

- The organization should use risk management techniques to determine (a) what system assets must be protected and to what level (e.g., applications, databases, "legacy" systems, devices, and connections) and (b) which remote user connections must be restricted. If a network is involved, what is its operational paradigm—that is, unicast (point-to-point network, such as Ethernet), multicast, or broadcast? An organization's answer will determine the type of access control product.
- What is the current infrastructure? Some products require the purchase of third-party applications, such as Relational Database Management Systems (RDBMS) (for storage of security databases) and Java server pages. The cost and complexity of the setup may be higher if these third-party applications are not already present.
- Role-based access control is most effective when roles closely reflect the actual hierarchy of the organization for which it will be used. For example, a senior human resources administrator may require assignment to multiple roles, whereas a clerk might only need the access associated with a single role. The cost and effort to engineer the roles should also be considered.
- Should sensitive security data, such as user access scripts, password data, etc., be stored and transmitted in the clear or encrypted form?
- What is the sensitivity of the protected network versus external network(s)? Is a trusted OS/trusted guard suggested?
- What is the direction of flow for which access control is required? Is it inbound/outbound or only inbound?
- Is there a single "super administrator" or support for delegation of authority to "subadministrators" with limited responsibility (e.g., user subsets or resource subsets)?
- What is the impact on the training and level of effort needed to identify and define roles, the organizational impact of implementing roles, and the responsibility for role maintenance?
- What are the procedures for adding and deleting users and adding/removing applications/resources in the organization?

### Product Considerations

- Which of the following access control method(s) does the product support and which is needed:
  - Internet Protocol (IP) address based
  - User identity-based
  - Group based
  - Role based (user authenticated and assigned a role, with access controlled based on that role).
- If the product supports access control based on defined rules, what is the granularity of the rules supported: access control per user, group, or role?
- What attributes or conditions of access are supported (e.g., type of transaction performed, time frame/frequency of transaction type, or physical/IP address origination)?
- Can the product limit specific transaction types (execution, creation, reading, writing, deletion and renaming) for a particular file or device types system wide or on selected components?
- Where is integration required—for example, types of applications, operating systems, etc.?
  - Some products support only Web applications or Web-enabled legacy applications, and then only certain applications without workarounds or modifications to application output.
  - What is the structure of the organization's existing user account directories and security databases?
  - To what level of granularity do the system's objects (e.g., files, directories/folders, components) need to be protected?
  - Can the access control product protect individual devices (e.g., floppy disks, compact disks–read-only memory [CD-ROM], serial and parallel interfaces, and system clipboard)?
- What is the logging capability for audit purposes?
- What is the complexity of installation, configuration, and use of the product's system administration function?
  - Does the product provide for easy definition and editing of access control rules, and of user/group permissions/accounts?
  - Does the product support remote administration?
  - Does it have a Hypertext Markup Language (HTML)/browser-based administrative interface or other graphical user interface (GUI)?
- Can the product support the enterprise's PKI/token/certificate authentication method?

- Is the product limited to supporting certain kinds of security rules/user account databases/directories (e.g., Lightweight Directory Access Protocol [LDAP]-only, X.500-only, or specific RDBMS brand name)?
  - Will the product work with current directories (e.g., LDAP, X.500) to store rules logic and user account information, or does it use a proprietary database or third-party RDBMS (if so, which ones)?
  - If the former, are any changes needed to the directory schema to accommodate additional security content? If the latter, is the database bundled with the system, or must it be purchased separately?
  - How transparent is the security rules/user account database made to the systems administrator by the security administrative application?
  - Does a feature exist that enables the database to automatically import user account information from existing directories?
  - If the organization will be using existing account directories with the product, what are the performance and security implications if directories are regularly shadowed/replicated?
- Can the product interoperate with security domains and databases on other systems?
- Is support for remote user access required?
- What support does the product provide for laptops/notebooks, personal digital assistants (PDA), and IP-based phones?
- Is the product centralized (e.g., central security server) or distributed (e.g., agent based, client proxy based)? Are changes required to servers or clients? If the product is agent based, will all systems in the organization require agents?
- Is the product integrated with an intrusion detection system (IDS) and/or firewall to enable automated (preprogrammed) access changes (e.g., intruder lockout) based on perceived potential malicious events?
- Are there mechanisms for immediate dissemination and implementation of access right changes?
- What is the requirement for support of component-level redundancy (with hot switchover to backup in case of failure) and scalability to accommodate growing enterprise/user base?
- Is there support for predeployment testing and verification of access rules?
- Are any standard application programming interfaces (API) provided for extensibility and integration with other tools (e.g., C++, C, and Java)? Must APIs be purchased from or custom developed by the vendor?
- Are other security functions provided (e.g., virus scanning, integrity controls, user, and password management)?

- Can the product encrypt and decrypt the transmission of files and directories? Will the product allow secure socket layer (SSL) encryption between a client browser and a security server so that no encryption is required on the backend systems being protected?
- Can the system protect against unauthorized access by use of an image versus presentation of an actual biometric object (i.e., presentation of a picture of an iris/retina versus presentation of the actual eye)?

## 5.3 Intrusion Detection

Intrusion detection is the process of monitoring events occurring in a computer system or network and analyzing them for signs of *intrusions*, defined as attempts to perform unauthorized actions, or to bypass the security mechanisms of a computer or network. Intrusions are caused by any of the following: attackers who access systems from the Internet, authorized system users who attempt to gain additional privileges for which they are not authorized, and authorized users who misuse the privileges given them. Intrusion detection systems (IDS) are software or hardware products that assist in the intrusion monitoring and analysis process.

The implementation of an IDS might be valuable for the following reasons:

- Prevent problem behaviors by increasing risk of discovery and punishment for system intruders
- Detect attacks and other security violations that are not prevented by other security measures
- Detect preambles to attacks (network probes and other tests for existing vulnerabilities)
- Document the existing threat to the organization
- Quality control for security design and administration
- Provide useful information about methods used in intrusions.

There are two different approaches to analyzing events to detect attacks: signature-based detection and anomaly detection. Either or both of the approaches could be used in an IDS product.

**Signature-Based Detection**[7]. This approach identifies events or sets of events that match with a predefined pattern of events that describe a known attack. These patterns are called signatures. Signatures may include system states, or accessing system areas that have been explicitly identified as “off-limits.”

**Anomaly Detection**. Anomaly detection assumes that all intrusive activities deviate from the norm. These tools typically establish a normal activity profile and then maintain a current activity profile of a system. When the two profiles vary by statistically significant amounts, an intrusion attempt is assumed.

NIST Special Publication 800-31, *Intrusion Detection Systems*, provides a more complete description and discussion of the important issues that should be considered when acquiring an IDS.

[7] Signature-based detection is sometimes referred to as misuse detection. Misuse detection is more explicitly defined as detecting insiders who abuse privileges given them.

### 5.3.1 Types of Products

Three common types of IDS products are network based, host based, and application based. Each type of product may optionally offer intrusion prevention capabilities.

**Network-Based IDS**. These IDSs detect attacks by capturing and analyzing network packets. Listening on a network segment or switch, one network-based IDS can monitor the network traffic affecting multiple hosts that are connected to the network segment.

Network-based IDSs often consist of a set of single-purpose sensors or hosts placed at various points in a network. These units monitor network traffic, performing local analysis of that traffic and reporting attacks to a central management console. Because the sensors are limited to running the IDS, they can be more easily secured against attack. Many of these sensors are designed to run in "stealth" mode, making it more difficult for an attacker to determine their presence and location.

**Host-Based IDS**. Host-based IDSs operate on information collected from within an individual computer system. This vantage point allows host-based IDSs to determine exactly which processes and user accounts are involved in a particular attack on the OS. Furthermore, unlike network-based IDSs, host-based IDSs can more readily "see" the intended outcome of an attempted attack, because they can directly access and monitor the data files and system processes usually targeted by attacks.

Host-based IDSs normally use information sources of two types: operating system audit trails, and system logs. Operating system audit trails are usually generated at the innermost (kernel) level of the operating system; therefore these trails are more detailed and better protected than system logs. Some host-based IDSs are designed to support a centralized IDS management and reporting infrastructure that can allow a single management console to track many hosts. Others generate messages in formats that are compatible with network management systems.

**Application-Based IDS**. Application-based IDSs are a special subset of host-based IDSs that analyze the events transpiring within a software application. The most common information sources used by application-based IDSs are the application's transaction log files.

The ability to interface with the application directly, with significant domain or application-specific knowledge included in the analysis engine, allows application-based IDSs to detect suspicious behavior due to authorized users attempting to exceed their authorization. This is because such problems are more likely to appear in the interaction among the user, the data, and the application.

**Intrusion Prevention**. Intrusion detection systems often have intrusion prevention capabilities. This means that not only can they detect an intrusive activity, but they can also attempt to stop the activity, ideally before it reaches its targets. Intrusion prevention is much more valuable than intrusion detection because intrusion detection simply observes events without making any effort to stop them. Unfortunately, intrusion prevention can also cause operational issues because if the detection of incidents is not accurate, then it may block legitimate activities that are incorrectly classified as malicious. Any organization that wants to utilize intrusion prevention should pay particular attention to detection accuracy when selecting a product.

Another consideration involving intrusion prevention is architecture-related. IDS products may be simply monitoring activity, or they may actually be "in-line", which means that activity must pass

through them. Examples include a network-based IDS that is integrated with a firewall and a host-based IDS that is integrated into the kernel of the operating system. An in-line intrusion detection system has the ability to block all detected attacks. If an IDS product is not in-line, its ability to block attacks may be limited.

### 5.3.2 Intrusion Detection Product Characteristics

An effective IDS should:

- Be easy to operate
- Be tunable to various parameters
- Run continually
- Be fault tolerant
- Resist subversion
- Impose minimal overhead on the system
- Observe deviations from normal behavior
- Be easily tailored to the system in question
- Cope with changing system behavior over time as new applications are being added
- Be easily maintained
- Be based on proven systems that provide periodic IDS signature updates
- Be able to log events to a secure location and be able to send alert messages to the appropriate security administrators
- Facilitate efficient intrusion analysis, incident handling and forensics
- Make logs easy to access and view
- Provide log filtering to allow easy manipulation and searching.

### 5.3.3 Environment Questions

#### Organizational Considerations

- Is the system compatible with the organization's current security architecture?
- Does the organization want to use the output of its IDS to determine new security requirements?
- Does the organization want to use the IDS to maintain managerial control (nonsecurity related) over system or network usage?
- What is the budget for acquisition and life cycle support of intrusion detection hardware, software, and infrastructure, including staffing to monitor and respond to intrusions?

### Product Considerations

- Is the product sufficiently scalable for your present and projected environment?
- Has the product been tested—against functional requirements and against attack?
- What is the level of expertise required by operators of the product?
- Is the product designed to evolve as the organization grows?
  - Can the product adapt to growth in security administrator expertise?
  - Can the product adapt to growth and change of the organization's systems infrastructure?
  - Can the product adapt to a changing threat environment?
- What are the general support requirements for the product?
- What support will the vendor provide for product installation and configuration support?
- What is the vendor commitment for ongoing product support?
  - Are subscriptions to signature updates included?
  - How often are subscriptions updated?
  - How quickly after a new attack is made public will the vendor ship a new signature?
  - Are software updates included?
  - How quickly will software updates and patches be issued after a problem is reported to the vendor?
  - Are technical support services included, and if so, what is the vendor's commitment to timely response?
  - What alternatives does the vendor offer for contacting technical support (e.g., e-mail, telephone, online chat, and Web-based reporting)?
  - Are there any guarantees associated with the IDS?
  - What training resources does the vendor provide as part of the product?
  - What additional training resources are available from the vendor and at what cost?

## 5.4 Firewall

Firewalls are devices or systems that control the flow of network traffic between networks or between a host and a network. A firewall acts as a protective barrier because it is the single point through which communications pass. Internal information that is being sent can be forced to pass through a firewall as it leaves a network or host. Incoming data can enter only through the firewall. This section is drawn from NIST Special Publication 800-41, *Guidelines on Firewalls*

*and Firewall Policy*. This publication provides details of firewalls and firewall product selection that are beyond the scope of this document.

While firewalls and firewall environments are often discussed in the context of Internet connectivity, firewalls have applicability in network environments beyond Internet connectivity. For example, many corporate enterprise intranets employ firewalls to restrict connectivity to and from internal networks servicing more sensitive functions, such as the accounting or personnel department. By employing firewalls to control connectivity to these areas, an organization can prevent unauthorized access to the respective systems and resources within the more sensitive areas. The inclusion of an internal firewall environment can therefore provide an additional layer of security that would not otherwise be available.

Although firewalls afford protection of certain resources within an organization, there are some threats that firewalls cannot protect against: connections that bypass the firewall, new threats that have not yet been identified, and viruses that have been injected into the internal network. It is important to remember these shortcomings because considerations will have to be made in addition to the firewall in order to counter these additional threats and provide a more comprehensive security solution.

### 5.4.1 Types of Products

NIST Special Publication 800-41 describes eight kinds of firewall platforms: packet filter firewalls, stateful inspection firewalls, application proxy gateway firewalls, dedicated proxy firewalls, hybrid firewall technologies, network address translation, host based firewalls, and personal firewalls/personal firewall appliances.

**Packet Filter Firewalls**. The most basic firewall is called a packet filter. Packet filter firewalls are routing devices that include access control functionality for system addresses and communication sessions. The access control functionality of a packet filter firewall is governed by a set of directives collectively referred to as a ruleset.

Packet filter firewalls have two main strengths: speed and flexibility. Packet filter firewalls can be used to secure nearly any type of network communication or protocol. This simplicity allows packet filter firewalls to be deployed into nearly any enterprise network infrastructure. Note that their speed, flexibility, and capability to block denial-of-service and related attacks make them ideal for placement at the outermost boundary with an untrusted network.

Packet filter firewalls possess several weaknesses:

- Because packet filter firewalls do not examine upper-layer data,[8] they cannot prevent attacks that employ application-specific vulnerabilities or functions.
- Because of the limited information available to the firewall, the logging functionality present in packet filter firewalls is limited. Packet filter logs normally contain the same information used to make access control decisions (source address, destination address, and traffic type).
- A firewall relying solely on packet filtering would not support advanced user authentication schemes.

[8] Above layer 3 in the Open Systems Interconnect (OSI) model: Transport (4), Session (5), Presentation (6), and Application (7).

- They are vulnerable to attacks and exploits that take advantage of flaws within the TCP/IP specification and protocol stack, such as network layer address spoofing.

Consequently, packet filter firewalls are very suitable for high-speed environments where logging and user authentication with network resources are not important.

An example of a packet-filter firewall is a network router employing filter rules to screen network traffic.

**Stateful Inspection Firewalls**. Stateful inspection evolved from the need to accommodate certain features of the TCP/IP protocol suite. When an application uses a TCP (connection-oriented transport) to create a session with a remote host system, a port is also created on the source system. This port receives network traffic from the destination system. Packet filter firewalls must permit inbound network traffic on all return packets from the destination system for connection-oriented transport to occur. Opening this many ports creates an immense risk of intrusion by unauthorized users who may employ a variety of techniques to abuse the expected conventions. Stateful inspection firewalls solve this problem by creating a directory of outbound TCP connections, along with each session's corresponding client port. This "state table" is then used to validate any inbound traffic. The stateful inspection solution is more secure because the firewall tracks client ports individually rather than opening all inbound ports for external access.

Stateful inspection firewalls share the strengths and weaknesses of packet filter firewalls, but because of the state table implementation, stateful inspection firewalls are generally considered to be more secure than packet filter firewalls.

Stateful inspection firewalls can accommodate other network protocols in the same manner as packet filters, but the actual stateful inspection technology is relevant only to TCP/IP. For this reason, many texts classify stateful inspection firewalls as representing a superset of packet filter firewall functionality.

**Application-Proxy Gateway Firewalls**. Application proxy gateway firewalls provide additional protection by inserting the application in the communications path, looking like the end-point of the communications to both sides of the firewall. For example, a web-proxy receives requests for external, web access from inside the firewall and relays them to the exterior web page as though the firewall was the requesting web client. The external web page responds to the firewall and the firewall forwards the response to the inside client as though the firewall was the web server. No through TCP/IP connection is ever made from inside client to external web server.

Application-proxy gateway firewalls have numerous advantages over packet filter firewalls and stateful inspection packet filter firewalls. First, application-proxy gateway firewalls usually have more extensive logging capabilities resulting from the firewall being able to examine the entire network packet rather than only the network addresses and ports.

Another advantage is that application-proxy gateway firewalls allow security administrators to enforce whatever type of user authentication is considered appropriate for a given enterprise infrastructure. Application-proxy gateways can authenticate users directly, as opposed to packet filter firewalls and stateful inspection packet filter firewalls, which normally authenticate users based on the network layer address of the system on which they reside (i.e., source, destination, and type). Given that network layer addresses can be easily spoofed, the authentication capabilities inherent in application-proxy gateway architecture are superior to those found in packet filter or stateful inspection packet filter firewalls.

The advanced functionality of application-proxy gateway firewalls also fosters several disadvantages when compared with packet filter or stateful inspection packet filter firewalls. First, because of the "full packet awareness" found in application-proxy gateways, the firewall is forced to spend significant time reading and interpreting each packet. Therefore, application-proxy gateway firewalls are not generally well suited to high-bandwidth or real-time applications. To reduce the load on the firewall, a dedicated proxy server can be used to secure less time-sensitive services, such as e-mail and most Web traffic. Another disadvantage is that application-proxy gateway firewalls are often limited in terms of support for new network applications and protocols. An individual, application-specific proxy agent is required for each type of network traffic that needs to transit a firewall. Most application-proxy gateway firewall vendors provide generic proxy agents to support undefined network protocols or applications. However, those generic agents tend to negate many of the strengths of the application-proxy gateway architecture, and they simply allow traffic to "tunnel" through the firewall.

**Dedicated Proxy Firewalls**. Dedicated proxy servers differ from application-proxy gateway firewalls in that they retain proxy control of traffic, but they do not contain firewall capability. They are typically deployed behind traditional firewall platforms for this reason. In typical use, a main firewall might accept inbound traffic, determine which application is being targeted, and then hand off the traffic to the appropriate proxy server (e.g., an e-mail proxy server). The proxy server typically would perform filtering or logging operations on the traffic and then forward it to internal systems. A proxy server could also accept outbound traffic directly from internal systems, filter or log the traffic, and then pass it to the firewall for outbound delivery.

Dedicated proxies allow an organization to enforce user authentication requirements and other filtering and logging on any traffic that traverses the proxy server. The implications are that an organization can restrict outbound traffic to certain locations or could examine all outbound e-mail for viruses or restrict internal users from writing to the organization's Web server. Security experts have stated that most security problems occur from within an organization; proxy servers can assist in foiling internally based attacks or malicious behavior. Simultaneously, filtering outbound traffic will place a heavier load on the firewall and increase administration costs. Many organizations enable the caching of frequently used Web pages on the proxy, thereby reducing firewall traffic. In addition to authentication and logging functionality, dedicated proxy servers are useful for Web and electronic mail (e-mail) content scanning.

**Hybrid Firewall Technologies**. Recent advances in network infrastructure engineering and information security have resulted in a "blurring of the lines" that differentiates the various firewall platforms discussed earlier. As a result, firewall products currently incorporate functionality from several different classifications of firewall platforms. For example, many packet filter or stateful inspection packet filter firewall vendors have implemented basic application-proxy functionality to offset some of the weaknesses associated with their firewall platform. In most cases, packet filter or stateful inspection packet filter firewall vendors implement application proxies to provide improved network traffic logging and user authentication in their firewalls. Nearly all major firewall vendors have introduced hybridization into their products in some manner; therefore it is not always a simple matter to decide which specific firewall product is the most suitable for a given application or enterprise infrastructure. Hybridization of firewall platforms makes the prepurchase product evaluation phase of a firewall project important. Supported feature sets, rather than firewall product classification, should drive the product selection.

**Network Address Translation**. Network address translation (NAT) technology was developed in response to two major issues in network engineering and security. Network address translation

is an effective tool for “hiding” the network-addressing schema present behind a firewall environment. In essence, NAT allows an organization to deploy an addressing schema of its choosing behind a firewall, while still maintaining an ability to connect to external resources through the firewall. Network address translation is accomplished by one of three methods: static, hiding, and port.

In static NAT, each internal system on the private network has a corresponding external, routable IP address associated with it. This particular technique is seldom used because of the scarcity of available IP address resources.

With hiding NAT, all systems behind a firewall share the same external, routable IP address. Thus, with a hiding NAT system, many systems behind a firewall will still appear as only one system. With port address translation, it is possible to place resources behind a firewall system and still make them selectively accessible to external users.

In terms of strengths and weaknesses, each type of NAT has applicability in certain situations, with the variable being the amount of design flexibility offered by each type. Static NAT offers the most flexibility, but as stated earlier, static NAT is not always practical given the shortage of IP version 4 addresses. Hiding NAT technology was an interim step in the development of NAT technology, but it is seldom used because port address translation offers additional features beyond those present in hiding NAT while maintaining the same basic design and engineering considerations. Port address translation is often the most convenient and secure solution.

**Host-based Firewalls.** Firewall packages are available in some OSs or as add-ons; they can be used to secure only the individual host. Internal servers should be protected and should not be assumed to be safe from attack because they are behind a main firewall. Host-based firewall packages typically provide access-control capability for restricting traffic to and from servers running on the host, and logging is usually available. A disadvantage to host-based firewalls is that they must be administered separately and maintaining security becomes more difficult as the number of devices to be configured increases.

**Personal Firewalls/Personal Firewall Appliances**. Securing personal computers (PC) at home or remote locations is now as important as securing them at the office; many personnel telecommute or work at home and operate on organization- or agency-proprietary data. Home users dialing an Internet service provider (ISP) may have limited firewall protections available to them because the ISP has to accommodate potentially many different security policies. Therefore, personal firewalls have been developed to provide protection for remote systems and to perform many of the same functions as larger firewalls. These products are typically implemented in one of two configurations.

The first configuration is a personal firewall, which is installed on the system it is meant to protect; personal firewalls usually do not offer protection to other systems or resources. Likewise, personal firewalls do not typically provide controls over network traffic that is traversing a computer network — they protect only the computer system on which they are installed.

The second configuration is a personal firewall appliance, which is in concept similar to a traditional firewall. In most cases, personal firewall appliances are designed to protect small networks such as networks that might be found in home offices. These appliances usually run on specialized hardware and integrate some other form of network infrastructure components in addition to the firewall itself, including the following: broadband modem wide area network

(WAN) routing, LAN routing (dynamic routing support), network hub, network switch, Dynamic Host Configuration Protocol (DHCP) server, Simple Network Management Protocol (SNMP) agent, and application-proxy agents.

In terms of deployment strategies, personal firewalls and personal firewall appliances normally address connectivity concerns associated with telecommuters or branch offices. However, some organizations employ these devices on the organizational intranet, practicing a layered defense strategy.

Management of the device or application is an important factor when evaluating or choosing a personal firewall or personal firewall appliance. Ideally, a personal firewall or personal firewall appliance should enable the organization or agency to enforce its defined security posture on all systems that connect to its networks and systems. In the case of telecommuters, this means that a personal firewall or personal firewall appliance should enforce a policy at least as restrictive as end-users would experience if they were behind the corporate or agency firewall in the office.

**Centrally Managed Distributed Firewalls.** The goals for host-based firewalls and personal firewalls/appliances can also be achieved using centrally managed distributed firewall products. All of these firewall types provide firewall capability in every protected computer. Centrally managed distributed firewalls are centrally controlled but locally enforced. A security administrator defines and maintains security policies, not the end-users. This places the responsibility and capability of defining security policies in the hands of a security professional who can properly lock down the target systems. A centrally managed system is scalable because each system does not have to be administered separately. A properly executed distributed firewall system includes exception logging. More advanced systems include location intelligence so that the appropriate policy is enforced depending on the context of the connection.

Centrally managed distributed firewalls can be either software- or hardware-based firewalls. Centrally managed distributed software firewalls are similar in function and features to host-based or personal firewalls, but the security policies are centrally defined and managed. Software distributed firewalls have the benefit of unified corporate oversight of firewall implementation on individual machines, however they remain vulnerable to attacks on the host operating system from the networks, as well as intentional or unintentional tampering by users logging into the system being protected.

Centrally managed distributed hardware firewalls combine the filtering capability of a firewall with the connectivity capability of a traditional connection. Filtering the data on the firewall hardware rather than the host system can make this system less vulnerable than software-based distributed firewalls. Hardware distributed firewalls can be designed to be unaffected by local or network attacks via the host operating systems. Performance and throughput of a hardware system is generally higher than software systems.

### 5.4.2 Firewall Product Characteristics

- A firewall environment should be employed to perform the following general functions:
  - Filter packets and protocols
  - Perform stateful inspection of connections
  - Perform proxy operations on selected applications

- Perform NAT
- Log traffic denied by the firewall

- The firewall should be able to filter packets based on the following characteristics:
  - Protocol (e.g., IP, Internet Control Message Protocol [ICMP])
  - Source and destination IP addresses
  - Source and destination ports (which identify the applications in use)
  - Interface of the firewall that the packet entered
- The proxy operations should, at a minimum, be operable on the content of Simple Mail Transfer Protocol (SMTP), File Transfer Protocol (FTP), and Hypertext Transfer Protocol (HTTP) traffic.

### 5.4.3 Environment Questions

#### Organization Considerations

- Organizations should use firewalls to secure their Internet connections and their connections to other networks. At remote locations, users should use personal firewalls or firewall appliances to secure their connections to the Internet and ISPs.
- Organizations should view firewalls as their first line of defense from external threats.
- Organizations must monitor incident response team reports and security Web sites for information about current attacks and vulnerabilities. The firewall policy should be updated as necessary. A formal process should be used for managing the addition and deletion of firewall rules.
- Organizations should recognize that all systems administration, especially firewall administration, requires significant time and training. Organizations should ensure that their administrators receive regular training to stay current with threats and vulnerabilities.
- Organizations should consider protecting individual systems that have a high risk of being attacked or becoming a launch point for an attack, or that house very sensitive or valuable data. Systems with public or outsider access, shared workstations, human resource and finance servers, and servers in a “demilitarized zone” fall into this category.
- Firewalls should run on a machine dedicated to that purpose.

#### Product Considerations

- What protocols are supported and/or filtered? Do they include the network-layer (packet/protocol filtering with ACLs), the application-layer (protocol/content filtering [virus checking, active code blocking]), or both?
- Is the organization currently reliant on products that employ protocols that are incompatible with firewall design and implementation (e.g., use of user datagram protocol [UDP] in a distributed database management system [DBMS])?

- Is the product a fully featured application-layer firewall or a firewall router with an ACL-driven packet filter?
- What types of ACLs are supported? Do they include basic (standard and static extended) or advanced ACLs?
- What are the basic ACL criteria: per interface, per network-layer protocol, per IP address and range, and inbound and outbound?
- What type of advanced access control is supported?
- What authentication servers and mechanisms are supported? Do they include TACACS/TACACS+/Extended TACACS, RADIUS, or other?
- How vulnerable is the firewall to attacks via the ne]twork against the firewall itself? If the firewall runs on an individual host for which all users are not trusted system administrators, how vulnerable is it to tampering by a user logged into the operating system running on the protected hosts?
- Does the system require end-users to configure and maintain security policies, security professionals to individually manage policies per host, or is the configuration centrally managed?
    - If centrally managed, how is this function secured?
    - If centrally managed, are remote systems with VPN connections covered by this feature?
- Can the firewall support hot-standby/failover/clustering?
- What type of NAT is supported?
- Is firewall "chaining" possible (to distribute filtering functions across a series, for better performance)?
- Is router-to-router authentication supported?
- Is there event logging and auditing?
- Is there router and firewall encryption?
- Is Internet Protocol security (IPSec) support available?
- If SNMP is addressable, does protection exist from an unauthorized administrator?
- Is the product SNMPv3 capable?

## 5.5 Public Key Infrastructure

The interconnectivity of networks and the Internet support opportunities for government and business to conduct electronic transactions. To enable these paperless business activities, it is critical to assure that the auditability and legal standing of these electronic transactions are comparable to the paper formats. One method of meeting this requirement is the use of public key technologies and a PKI.

A PKI can be quite complex. Similarly, the strategies for implementing a PKI may range from complete outsourcing of all functionality to building a homegrown PKI from COTS products. The nuances and details of PKI implementation strategies are well beyond the scope of this document. For a detailed treatment of the subject, the following references are highly recommended:

- NIST Special Publication 800-25, Federal Agency Use of Public Key Technology for Digital Signatures and Authentication
- NIST Special Publication 800-32, Introduction to Public Key Introduction to Public Key Technology and the Federal PKI Infrastructure
- The Federal Public Key Infrastructure Steering Committee Web site at http://www.cio.gov/fpkisc
- PKI information can be found at http://csrc.nist.gov/pki**.**

Discussion of the service aspects of PKI support is addressed in NIST Special Publication 800-35, *Guide to Information Technology Security Services*. This section briefly defines the key concepts of PKI and identifies key criteria for decision making to provide a means for developing an initial purchasing and implementation strategy.

**PKI Terms and Introduction.** Public key cryptography relies on the concept of a key pair, composed of a private key, which must be kept a secret, and a mathematically related public key. Common functions of public key cryptography are as follows:

- **Digital Signatures**. A key holder signs a digital document with a secret private key, and a relying party can verify that signature with the public key and know that the document has not been altered in any way since it was signed and that it was signed with the unique private key corresponding to the verification public key.
- **Exchange of Certificates.** Certificates containing access permissions and/or security attributes can be distributed using public key cryptography.
- **Exchange of Cryptographic Keys**. A relying party can use a public key to encrypt or agree to a secret symmetric key to be shared with the private key holder and used in a subsequent message or protocol to encrypt data.

PKI is a systematic means of managing key pairs and associating the names of key holders with their public keys. In a PKI, a trusted Certificate Authority (CA) issues public key certificates to subscribers (e.g., people, organizational entities, or even network devices), typically binding the subscriber's public key to the subscriber’s name and security and identity attributes. The certificate is digitally signed by the CA, and the public key of the CA can be known by all potential relying parties. Thus, a relying party can verify a subscriber's true public key by verifying the signature on the subscriber's certificate, and then relying on the subscriber's public key in subsequent e-commerce transactions. CAs rely on the services of a Registration Authority (RA) to vouch for the identity of subscribers and to publish certificates and certificate status information to a repository, which is usually a directory accessible via the LDAP protocol.

Subscribers and relying parties use PKI-enabled applications in actual e-commerce. These applications, in turn, use PKI clients to perform signing, verification, and key management operations. The digital signature and key management functionality of PKI are used in PKI-enabled applications to achieve authentication, integrity, confidentiality, and nonrepudiation.

### 5.5.1 Types of Products

Before selecting a CA product, a CA service provider, or PKI clients, an organization should understand the PKI-enabled applications that it wishes to run and the products available for those applications. In many cases, it will make sense to select the CA and client type in conjunction with the primary application packages, or to select the applications first and let them drive PKI choices. Once the applications to be supported have been identified and the security policies and requirements associated with them have been defined, the following characteristics will differentiate PKI products.

**Key Protection and Cryptographic Modules.** The protection afforded private keys is a major factor in establishing the assurance level of a PKI. Agencies should decide what their assurance requirements are and ensure that the kinds of modules needed to achieve that assurance are incorporated in CAs and clients. In most cases, PKI products can use a range of cryptographic modules, but all PKI products do not support all modules. Private keys should always be stored and used in an approved cryptographic module, validated to conform to FIPS 140-2. FIPS 140-2 has four levels of security, 1 to 4, in order of increasing security. The CA cryptographic module should normally be at levels 2 to 4 depending on the sensitivity of the data and transactions being protected. Hardware cryptographic modules are usually more secure than software-based products. In many cases, CAs and RAs will use hardware modules, and subscribers will use software modules, however in some cases many or all subscribers will also use hardware modules.

**Cross-Certification and the Federal PKI Architecture.** In some cases, organizations will wish to allow their users to use certificates issued by another CA to conduct business with other agencies and organizations. This action requires that the CA be capable of some form of cross-certification, where the CA can issue certificates to other CA's extending trust to that CA, its subscribers, and its associated applications. If this capability is required by the organization, it is critical that the products selected strictly adhere to industry standards. Demonstration of interoperability with a wide variety of CA vendors' products is recommended.

The Federal PKI Bridge CA (FBCA) provides a trust path between PKIs in various agencies. The use of it, however, depends on the use of clients capable of building certification paths of certificates through cross-certificates stored in directories. The FBCA defines certificate policies for four levels of assurance. Technical interoperation with the FBCA is the ability to process certain certificate extensions, including nameConstraint, certificatePolicies, and policyMapping. Agencies wishing to cross-certify with the bridge CA should ensure that the clients, CAs, and directory servers they select can interoperate technically with the Bridge CA and that the products selected support the policy requirements established for the level of assurance. Current policy and interoperability information is available at http://www.cio.gov/fpkisc/documents.

**Repositories.** CAs typically publish certificates and certificate revocation lists (CRL) to directory servers, and many clients can retrieve the certificates and CRLs they need from directories. Agencies may chose to implement a directory solely for the purposes of PKI, or they may integrate directories into a broad range of applications and services, including PKI. It is easier to build a directory solely for PKI, but also less generally useful.

The LDAP is used by CAs and clients to publish and retrieve certificates and CRLs. Directories are a complex subject in their own right; however, nearly all now support LDAP. A broad consideration of directory issues is beyond the scope of this section; however, agencies

implementing PKI should consider their directory plans and needs, and make PKI directory decisions in that broader context.

**Key Recovery.** Most CA products today offer a key recovery capability for encryption or key management private keys only. (If signature private keys are subject to key recovery, then nonrepudiation is compromised.) Although other key recovery schemes are possible, many CA products offer a feature in which the CA automatically keeps a backup copy of the encryption private key. This copy can be used to recover encrypted data if subscribers lose their keys, or are not available to activate their key. Agencies should consider key recovery needs when procuring CA products or PKI-enabled applications that encrypt stored data.

**Certificate Status.** Certificates may be revoked before they expire. Most CA products can create a list of revoked certificates called a certificate revocation list (CRL) and post it in a repository, and most clients can check such a list. The freshness of this revocation information may be an issue in a PKI; and the CRL features and capabilities of CAs products, services, and clients vary significantly, but support for these features in CA products and clients is not ubiquitous. A wide range of alternative means exists for tracking and managing certificate status in a PKI, each with its own efficiencies and weaknesses. Certificate status and revocation are major issues in the performance and scalability of PKIs and in the assurance level of certificates. The larger the PKI, the more difficult and expensive it is to maintain very fresh status information. High-assurance certificates, however, require a status mechanism that provides fast effective revocation to limit the damage caused by key compromises. Agencies selecting PKI products or services must determine their certificate status requirements. They also must select a system and products that can provide needed status information in a timely manner as the PKI grows in size and scope.

**PKI-Enabled Applications.** In a sense, the CA, the clients it supports and the entire PKI are "just plumbing." Perhaps the most basic elements to be considered in selecting a CA product or service provider are the applications that are enabled to use the clients supported by the CA. PKI enabled applications and products include the following:

- S/MIME secure E-mail application that can be used to sign and encrypt e-mail. The S/MIME software uses the subscriber's PKI client to perform PKI operations with certificates and keys.
- Web servers and browsers that implement the SSL/Transport Layer Security (TLS) are widely implemented and support not only PKI-based cryptographic authentication of servers and clients but also encryption of traffic in “secure” sessions. Again, the application either relies on a PKI vendor’s PKI client or uses a built-in PKI client to perform PKI operations.
- Document-signing products or applications that are used with forms, document management, or workflow products to allow signatures and approvals on electronic documents and to replace signed paper documents.
- Access control that uses certificates and a challenge/signed response protocol to authenticate an identity or privilege for use in access control, and may implement "single sign-on" for a variety or services.
- Products with built-in PKI-enabled access control—for example, firewalls, mail servers, or directory servers. These products often rely on the SSL/TLS protocol.
- File encryption systems that may use public key certificates to manage file encryption keys and to provide for a key recovery capability, if keys are otherwise lost.

### 5.5.2 PKI Product Characteristics

- The PKI product must be designed and implemented in a manner that ensures that the security policies can be enforced.
- The system should provide for easy key maintenance and secure public and private key backups.
- The selected PKI products must be compliant with applicable federal regulations and policies such as the following:
  - FIPS PUB 140-2: Security Requirements for Cryptographic Modules
  - FIPS PUB 180-2: Secure Hash Standard
  - FIPS PUB 186: Digital Signature Standard.
- The PKI product must conform to the X.509v3 or PKIX standards. These standards are the basis for most PKI-oriented products. If scalability and future interoperability are necessary requirements, products that conform to these standards should be considered.
- PKI client products must implement the PKIX path processing algorithm in conformance to X.509 and RFC 3280. Conformance is demonstrated by performing the PKITS X.509 path validation test suite, available at http://csrc.nist.gov/pki/testing/x509paths.html.

### 5.5.3 Environment Questions

**Organizational Considerations**

- How critical is the system in meeting the organization's mission?
- What regulations and policies are applicable in determining what is to be protected?
- What threats are applicable in the environment in which the system will be operational?
- What security and cryptographic objectives are required by the system (e.g., integrity, confidentiality)?
- Are users knowledgeable about PKI, and how much training will they undergo?
- The organization should establish objectives to be achieved by the PKI product and policies and procedures to support those objectives.
- The process of establishing a complete set of policies to support a PKI product can involve addressing numerous difficult issues, including privacy, maintaining assurance (trust) levels, key recovery, and long-term proof of identity and authenticity.
- Interconnection policies with other PKI products should be established.
- Are processes in place to ensure that required assurance levels do not degrade over time?
- Does the vendor or organization have policies for electronically archiving digitally signed documents, possibly for long periods of time?
- The organization must define the coverage of any licenses (e.g., enterprise wide, site specific) and document agreement.

- The organization should determine how difficult it is to migrate from one PKI product to another.
- What is the projected growth of the organization?
- What physical security measures are required to ensure the integrity of a central PKI solution?

### Product Considerations

- Is the product compatible and interoperable with other PKI products/service providers?
- Are there proprietary interface dependencies?
- What is the ease of supporting applications (e.g., virtual private networks, access control, secure e-commerce, smart card management, smart cards and hardware, directories, secure messaging, secure forms, and enterprise)?
- Is the product easy to deploy?
- What is the flexibility of administration?
- What is the scalability of installation?
- Does the vendor use interoperable products that fully conform to existing PKI standards?
- Will the organization's PKI product accept digital certificates from other PKI products?
- The system should provide for easy key maintenance and secure public and private key backups.
- A determination should be made regarding the maximum number of certificates that the organization would need and whether the service provider could accommodate that number.
- What is the level of effort required for application, database, and OS modification to support system?
- What encryption algorithms and certificate types are supported? Are they user selectable?
- Is there support for smart cards, PCMCIA tokens, etc.?

## 5.6 Malicious Code Protection

Viruses, worms and other malicious code[9] are typically hidden in software and require a host to replicate. Malicious code protection requires strict procedures and multiple layers of defense. Protection includes prevention, detection, containment, and recovery. Protection hardware and access-control software can inhibit this code as it attempts to spread. Most security products for detecting malicious code include several programs that use different techniques.

### 5.6.1 Types of Products

**Scanners**. Scanners provide precise identification of known malicious code. Scanners search for "signature strings" or use algorithmic detection methods to identify known code. Scanners rely on

[9] The terms "virus" and "malicious code" are used interchangeably in this section.

a significant amount of a prior knowledge about the code. Therefore, it is critical that the signature information for scanners is current. Most scanners can be configured to automatically update their signatures from a designated source, typically on a weekly basis; scanners can also be forced to update their signatures on demand.

**Integrity Checkers**. Integrity checkers detect infections by searching a program or other executable code to determine if it has been altered or changed. Integrity checkers can only flag a change as suspicious; they cannot determine if the change is a genuine virus infection. These programs are usually checksum based. The integrity checking process begins with the creation of a baseline, where checksums for clean executables are computed and saved. Each time the integrity checker is run, it again makes a checksum computation and compares the result with the stored value. Note that several different kinds of checksums are used. Simple checksums are easy to defeat; cyclical redundancy checks (CRC) are better, but can still be defeated. Cryptographic checksums such as SHA provide the highest level of security.

**Vulnerability Monitors**. These monitors are designed to prevent modification or access to particularly sensitive parts of the system; consequently, the monitors may block an attack on those parts. This requires considerable information about "normal" system use because PC viruses typically take advantage of system vulnerabilities and do not circumvent any security features. This type of software also requires decisions from the user about permitted operations.

**Behavior Blockers**. These programs contain a list of rules that a legitimate program must follow. If the program breaks one of the rules, the behavior blockers alert the users. The "sandbox" concept is that untrusted code is first checked for improper behavior. If none is found, it can be run in a restricted environment, where dynamic checks are performed on each potentially dangerous action before it is permitted to take effect. By adding multiple layers of reviews and checks to the execution process, behavior blockers can prevent malicious code from performing undesirable actions.

### 5.6.2 Malicious Code Protection Product Characteristics

- Accuracy, ease of use, administration, and system overhead should be considered in product selection.
- Virus protection products should be procured from vendors with a history of frequent updates and swift responses to new viruses.
- The product should be able to update virus definitions on demand and automatically on a pre-set schedule. The product should be configurable so that virus definition updates can be downloaded to a central host within the organization and that individual clients can be configured to acquire their updates from that host.
- The tool should be able to perform an automatic scan of the hard drive for viruses and to check the memory at the frequency level required by the organization's perceived risk level.
- The tool should be able to protect the boot record.
- The tool should provide an option to choose scanning preferences and perform on-demand scans.
- The tool should be able to provide real-time protection, scanning all files that are opened, created or downloaded. This includes protecting incoming data from modems, network

connections, PDAs and other removable devices so that viruses can be intercepted before they are stored on the hard drive.

- Integration with e-mail, Web, FTP, instant messaging and other applications that may transport malicious code should be transparent but effective.
- The tool should be able to scan all file types for malicious code and monitor JavaScript and ActiveX components for malicious activity.
- The tool should inform the user when a virus is detected and prompt the user to select an appropriate action, such as deleting an infected file or attempting to remove the virus from an infected file.
- The tool should offer a repair feature of any infected files or quarantine files designated as irreparable.

### 5.6.3 Environment Questions

#### Organizational Considerations

- Are systems connected to an internal or external network? Are there other network controls in place (e.g. a firewall on an internal network)?
- Are system components known to be vulnerable to attack (e.g., email and browser applications)?
- Is transportable storage media brought in from outside sources?

#### Product Considerations

- Can the user perform an update of virus definition files whenever needed?
- Can the administrator force an update?
- Does the product support all operating systems (OS) (e.g., Linux/UNIX mail servers) in the organization?

#### Vendor Considerations

- What level of support is available to the end-user?
- Is the vendor able to develop and publish virus signatures in a timely manner? Do vendors develop their own virus signatures, or are the signatures based on published search strings?
- What is the level of documentation needed?
- Can the vendor create custom virus definitions for the organization?

## 5.7 Vulnerability Scanners

Vulnerability scanners examine hosts such as servers, workstations, firewalls and routers for known vulnerabilities. Each vulnerability presents a potential opportunity for attackers to gain unauthorized access to data or other system resources. Vulnerability scanners contain a database of vulnerability information, which is used to detect vulnerabilities so that administrators can mitigate through network, host and application-level measures before they are exploited. By

running scanners on a regular basis, administrators can also see how effectively they have mitigated vulnerabilities that were previously identified. Products use dozens of techniques to detect vulnerabilities in hosts' operating systems, services and applications.

### 5.7.1 Types of Products

**Network Vulnerability Scanners**. Network vulnerability scanners are utilized to detect vulnerabilities on remote hosts by performing scans across networks. These scanners typically identify only those vulnerabilities that can be exploited remotely. Most network vulnerability scanners first perform network mapping to enumerate the hosts, then send additional scans and probes to each host to fingerprint its operating system and identify the applications and services it is running. The final step is to examine each application and service for known vulnerabilities. Some tools take this a step farther and actually attempt to validate the identified vulnerabilities by exploiting them; this is known as penetration testing.

**Host Vulnerability Scanners**. Host vulnerability scanners are run on a particular host to detect its vulnerabilities. These scanners identify vulnerabilities that can be exploited either remotely or locally. Typically the administrator defines security policy settings for each operating system in use, and the scanner compares the policies to the actual settings of each host. Host vulnerability scanners usually identify vulnerabilities primarily by checking configuration settings and user and group-related information, including permissions and ownership.

**Outsourced Scanning**. An alternative to acquiring vulnerability scanning is to contract with an outside vendor to perform the scanning. An outside vendor uses the same host and network scanners that individual organizations may have, but the vendors can typically possess a wide range of open source and commercial products, a deep knowledge of vulnerabilities and scanning techniques, and more experience in performing vulnerability scans, increasing the likelihood of detecting vulnerabilities. On the other hand, the vendors typically lack the specific knowledge of an organization's environment that is needed to determine the significance of vulnerabilities. Outsourced scanning works best when the security, network and system administrators within an organization collaborate with the vendor. Outsourced scanning is also often extended into a full penetration test to determine not only what vulnerabilities exist within an environment, but how attackers may exploit them.

### 5.7.2 Vulnerability Scanner Product Characteristics

- Accuracy, ease of use, administration and system overhead should be considered in product selection.
- The tool should be easily customizable for an environment and for particular hosts within the environment.
- Vulnerability scanners should be procured from vendors with a history of frequent updates and rapid responses to new serious vulnerabilities.
- The product should be able to update its vulnerability database from remote locations or local files, on demand and automatically on a pre-set schedule.
- The tool should provide an option to choose scanning preferences such as intensity and speed so that scanning does not overwhelm hosts, networks or the scanner itself.
- The tool should minimize host crashes, lockups and other problems inadvertently caused by scanning activities.

- The tool should determine for each host which ports are listening and what application or service is listening at each port. It should not make any assumptions regarding which services or applications are listening at a particular port number.
- The tool should use a combination of methods to identify vulnerabilities. The methods used will vary from product to product and are also dependent on whether host or network scanning is being performed and on the operating system of the target. Possible methods include:
  - Permission and ownership checks on files, directories, shares, Windows registry settings and other components
  - Reviewing user and group privileges and group membership
  - Password, screen saver, remote access, logging and audit policy checking
  - Banner grabbing, to identify service and application types and versions, and to confirm that legal notices are provided before access is granted
  - Password guessing, particularly default operating system and application accounts and passwords.
  - The results produced by the tool should be easy to view and to compare with previous results.
  - Whenever applicable, the tool should report the CVE number for each identified vulnerability.
  - The tool should make specific recommendations for mitigating each identified vulnerability and provide references to additional information.
  - The tool should report a reasonable risk level for each vulnerability.

### 5.7.3 Environment Questions

#### Organizational Considerations

- Can the product scan systems that are at high risk of being attacked more frequently than others?
- Can the product integrate vulnerability scanning with existing patch management practices? For example, it may be desirable to scan systems immediately before and after patches are applied to confirm that the patches have resolved the vulnerabilities and that the patching process has not inadvertently introduced additional vulnerabilities into the systems.
- Has the organization ensured that intrusion detection analysis and incident response personnel are made aware of all vulnerability scanning activity so that they do not misinterpret alerts and log entries as indications of an attack?

#### Product Considerations

- Can the administrator perform an update of the scanner’s vulnerability database whenever needed?

- Does the product support all operating systems of interest (e.g. Windows, Unix, Linux, Cisco IOS) in the organization?
- Can the administrator create custom vulnerability database definitions?
- Can intrusion detection systems be configured to ignore activity that is generated by authorized scanner operation? If not, can the scanner be configured to operate slowly enough so that the intrusion detection systems do not malfunction due to a flood of scanner-triggered alerts?
- For host vulnerability scanners, does the product require agents to be installed on each host? If so, how are the individual agents managed and updated?
- Can the product fix certain vulnerabilities that it identifies? If so, can it be configured to fix vulnerabilities automatically or to require manual approval of each action?
- If the product is capable of exploiting vulnerabilities, can it be configured to not attempt to do so?
- Where and how are the results of the scans stored? Is access restricted to only authorized administrators and security personnel?

### Vendor Considerations

- What level of support is available to the personnel performing the scanning?
- Does the vendor develop and publish new vulnerability database entries in a timely manner?
- Can the vendor create custom vulnerability database definitions for the organization?
- Does the vendor charge a flat fee and/or a fee for each scanned host or IP address?
- What is the level of documentation needed?

## 5.8 Forensics

Computer forensics involves the identification, preservation, extraction, and documentation of computer-based evidence.[10] Such information may be hidden from view; thus, special forensic software tools and techniques are required. Forensic software tools and methods can be used to identify passwords, log-ons, and other information that may have been deleted from the computer memory. These tools can also be used to identify backdated files and to tie a diskette to the computer that created it.

The computer forensics process consists of three phases: acquisition, examination, and presentation. Computer forensic investigators must have software tools that can effectively and efficiently accomplish the following tasks:

- Image data (e.g. make a clone of suspect media)
- Create comprehensive file listings with file checksums
- Compare an existing list of file checksums with the checksums of current files

[10] http://www.cybercrime.gov describes the Federal Criminal Code as it relates to the search and seizure of computers and the gathering of electronic evidence.

- Identify and recover text located anywhere on the storage media
- View text and image files
- Assure that recovery methods do not unnecessarily contaminate data evidence or produce artifacts
- Identify compressed data and decompress it
- Identify files by their contents and file header signatures, not just filenames and file extensions
- Identify encrypted files.

### 5.8.1 Types of Products

Forensic tools can be purchased individually or as a suite. They may be grouped into two categories: evidence preservation and collection tools, and analysis tools. These tools facilitate many different forensic activities, including evaluating system content, file comparisons, transactions, and file deletions.

**Evidence Preservation and Collection Tools**. These tools preserve the integrity of data that resides on evidentiary computer media and provide an unobtrusive mechanism for making copies of some or all of the original data. Write-protection tools and disk imaging software assist forensic examiners during preservation and copying of evidence.

**Analysis Tools**. The primary function of forensic analysis tools is to assist the examiner in analyzing vast amounts of data. Analysis tools perform the following:

- Recover deleted files
- Recover data not allocated to a specific file or application
- Perform string and pattern matching
- Conduct file identification
- Perform file listing or cataloging.

### 5.8.2 Forensics Product Characteristics

The needed characteristics of a computer forensic toolset will vary with each application. Some products perform a wide range of forensic tasks, such as text string search, deleted file recovery, free space extraction, and hidden data recovery, while others perform only a single task.[11]

### 5.7.3 Environment Questions

#### Organizational Considerations

- Does the organization need to analyze evidence from a computer incident?

[11] We advise close consultation and coordination with legal and law enforcement officials if forensic activities are undertaken where criminal or civil investigation or litigation is a potential outcome.

- Does the organization need to recover data from computers seized as evidence and to present it to law enforcement for investigative use and to prosecutors for use at trial?
- Is the acquisition and analysis of the media performed by the same individual?

### Product Considerations

- Will the product find data on all applicable file systems (e.g. FAT12 (floppy disks), FAT16 (Win3.x, Win95), FAT32 (Win98), NTFS (WinNT), NTFS5 (Win2000), HFS and HFS+ (Macintosh), Ext2FS and Ext3FS (Linux), UFS (Solaris), FFS (Unix), virtual file systems)?
- Is the product designed to be used with the OS in use at the organization?
- Does the product analyze large hard disk partitions and very large hard drives in use by the organization?
- Does the product have reporting capabilities? Does it have case management and configuration management capabilities?
- Does the product prevent the modification of evidence?
- What media does the product support? (e.g., floppy, CD-ROM, optical, tape, and other drives in use by the organization)?
- What is the speed of duplication/collection?
- Does the product sanitize the destination media prior to duplication/collection?

## 5.9 Media Sanitizing

With the more prevalent use of increasingly sophisticated encryption systems, an attacker wishing to gain access to an organization's sensitive data is forced to look elsewhere for information. One avenue of attack is the recovery of supposedly deleted data from media or memory. This residual data may allow unauthorized individuals to reconstruct and thereby gain access to sensitive information. Media sanitization tools can be used to thwart this attack by ensuring that deleted data are completely removed from the system or media.

When storage media are transferred, become obsolete, or are no longer usable as a result of damage, it is important to ensure that residual magnetic, optical, or electrical representation of data that has been deleted is no longer recoverable. Sanitization is the process of removing data from storage media, such that there is reasonable assurance, in proportion to the sensitivity of the data, that the data may not be retrieved and reconstructed. Once the media are sanitized, it should be impossible or impractical to retrieve the data. There are several accepted methods for sanitizing media: overwriting, degaussing, and destruction[12].

### 5.9.1 Types of Products

- **Overwriting**. One method to sanitize media is to use software or hardware products to overwrite storage space on the media with nonsensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) to be erased or deleted but also the entire media, including all addressable locations. The security

[12] The cost and benefit of a media sanitization method should be understood prior to a final decision. For instance, it may not be cost effective to degauss inexpensive media like diskettes.

goal of the overwriting process is to replace sensitive data with nonsensitive random data. Media should be overwritten a minimum of three times using a method based on the information sensitivity contained on the media. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method.

- **Degaussing**. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can erase. Degaussers have two different mechanisms: strong magnet and electromagnetic. Degaussing can be an effective method for sanitizing damaged media, for sanitizing media with exceptionally large storage capacities, or for quickly sanitizing diskettes. Degaussing is not effective for sanitizing nonmagnetic media, such as optical media.

- **Destruction**. Media also can be sanitized using physical destruction of the media. Physical destruction can be accomplished using a variety of methods, including disintegration, incineration, pulverization, shredding, melting, sanding, and acid bath. Physical destruction may be the only appropriate sanitization method for optical media, such as CD-ROM (read only) and Write-Once Read-Many (WORM).

  – *Disintegration, Pulverization, Melting, and Incineration.* These sanitization methods are designed to completely destroy the media. They are typically conducted at an outsourced metal destruction or incineration facility with the specific capabilities to perform these activities effectively, securely, and safely.

  – *Shredding.* Paper shredders can be used to destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should small enough that there is reasonable assurance in proportion to the sensitivity of the data that the data cannot be reconstructed.

  – *Sanding.* Sanding is the application of an abrasive substance (e.g., an emery wheel, grinder, or disk sander or sanding device) to the media's physical recording surface. The entire media recording surface must be removed completely.

  – *Acid Bath.* The application of acid solutions (e.g., concentrated hydriodic) to the media is typically conducted at an outsourced facility with the specific capabilities to perform these activities effectively, securely, and safely.

- **Memory Sanitization.** Sanitization of memory is determined based on whether the memory is volatile or nonvolatile. Volatile memory, such as RAM chips, requires power to maintain their content. Removing electrical power from the chip will erase or sanitize its contents. Nonvolatile memory, such as forms of Programmable Read-Only Memory (PROM) flash memory, maintain their contents permanently or until reprogrammed. Sanitization methods vary for specific forms of PROM. These methods include ultraviolet light, PROM programmers using overwriting, and physical destruction.

### 5.9.2 Media Sanitizing Product Characteristics

#### Overwriting

- Can overwrite disks regardless of the OS used to write them originally

- Overwrites an entire physical drive regardless of the types or lack of partitions
- Can overwrite logical file locations
- Notification is provided or recorded when address space cannot be overwritten
- Overwrite method and number of repetitions is configurable (e.g. using static or dynamic data)
- Provides a capability to verify or inspect the overwrite
- Does not damage the media.

#### Degaussing[13]

- Tested to verify degaussing capabilities (e.g., Type I, low energy; Type II, high energy)
- Does not damage the media.

#### Destruction

- Conducted at an approved facility or location, whether performed internally by the organization or outsourced, that has been proved effective, secure, and safe.

#### Shredders

- Crosscut or stripper
- Shred size of refuse meets appropriate standards based on the sensitivity of the data stored on the media.

#### Sanding

- Uses an approved abrasive substance, such as an emery wheel, grinder, disk sander, or sanding device
- Conducted at an approved facility or location, whether performed internally by the organization or outsourced, that has been proved effective, secure, and safe
- The entire recording media surface is removed completely.

### 5.9.3 Environment Questions

#### Organizational Considerations

- What types (e.g., optical nonrewritable, magnetic) and size (e.g., megabyte, gigabyte, and terabyte) of media storage does the organization require to be sanitized?
- What is the sensitivity of the data stored on the media?
- Will the media be processed outside a controlled area?
- Should the sanitization process be conducted within the organization or outsourced?

[13] The cost versus benefit of a media sanitization method should be understood prior to a final decision. For instance, it may not be cost effective to degauss a inexpensive media like diskettes.

- What is the anticipated volume of media to be sanitized by type of media?

### Product Considerations

- Is the media storage volatile or nonvolatile?
- Is the sanitization method appropriate for the media type, data sensitivity, and organization?

## Appendix A–References

National Institute of Standards and Technology (NIST). *Special Publication (SP) 800-12: An Introduction to Computer Security: The NIST Handbook*. October 1995.

NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*. September 1996.

NIST SP 800-21, *Guidelines for Implementing Cryptography in the Federal Government*. November 1999.

NIST SP 800-23, *Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*. August 2000.

NIST SP 800-25, *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*. October 2000.

NIST SP 800-27, *Engineering Principles for Information Technology Security: A Baseline for Achieving Security*. June 2001.

NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, January 2002.

NIST SP 800-31, *Intrusion Detection Systems*. August 2001.

NIST SP 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*. February 2001.

NIST SP 800-33, *Underlying Technical Models for Information Technology Security*. December 2001.

NIST SP 800-35, *Guide to Information Technology Security Services*, October 2003.

NIST SP 800-41, *Guidelines on Firewalls and Firewall Policy*. January 2002.

NIST SP 800-51, *Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme*, September 2002.

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems,* draft.

NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle*, October 2003.

Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, June 2001.

FIPS 180-2, *Secure Hash Standard (SHS)*, August 2002.

FIPS 186-2, *Digital Signature Standard (DSS)*, January 2000.

NIST Computer Security Laboratory Bulletin: *Disposition of Sensitive Automated Information*. October 1992.

Federal Information Security Management Act of 2002, 44 U.S.C. Chapter 35, Subchapter III. 2002.

United States *Federal Acquisition Regulation*. September 2001.

U.S. Office of Management and Budget. *Circular A-130, Appendix III: Security of Federal Automated Information Resources*. November 28, 2000.

U.S. Department of Energy, Federal Energy Regulatory Commission. *Information Technology Security Solutions Evaluation and Review*. June 11, 2001.

U.S. Navy Staff Office. *NAVSO Publication 5239-26: Remanence Security Guidebook.*

U.S. Department of Energy. *Clarification to the DOE Manual 5639.6A-1: Clearing, Sanitizing, and Destruction of Automated Information Systems Storage Media, Memory, and Hardware.* December 30, 1996.

Defense Technical Information Center - Information Assurance Technology Analysis Center. *Computer Forensics: Tools & Methodology, Critical Review and Technology Assessment Report.* Michael Noblett, Adam Feldman. May 12, 1999.

Defense Technical Information Center - Information Assurance Technology Analysis Center. *Information Assurance Tools Report, Intrusion Detection.* June 15, 2001.

U.S. Critical Infrastructure Assurance Office. *Practices for Securing Critical Information Assets.* January 2000.

U.S. General Services Administration. *A Guide to Planning, Acquiring, and Managing Information Technology Systems.* December 1998.

National Computer Security Center. *NCSC-TG-025, Version-2: A Guide to Understanding Data Remanence in Automated Information Systems*. September 2, 1991.

David F. Ferraiolo, D. Richard Kuhn, Ramaswamy Chandramouli. *Role-Based Access Control.* Artech House, 2003.

Rita Summers. *Secure Computing: Threats and Safeguards*. McGraw Hill, 2000.

Gartner Group. *Biometrics-Based Recognition for Financial Services, Context Overview Report*. December 31, 1998.

Jim Rapoza. *Accessing Control*. eWeek.com. December 4, 2000.

Jim Rapoza. *Access Control Tools Add Site Security*. eWeek.com. July 17, 2000.

Steve Lewis, Steve Wilson, and Martin D'Cruze. *Why do you want web access control anyway?/Interactive scorecard and NetResults: Web access control packages*. Network World. May 28, 2001.

Jay Bellamy. *Knock Knock, Who's There?* InfoSecurity/Secure Computing. March 2001.

Rutrell Yasin. *Access Control Gets Granular*. InternetWeek. January 20, 2000.

The Biometrics Consortium. <http://www.biometrics.org>.

The Common Criteria Project. < http://www.commoncriteria.org >.

The Smart Card Industry Association. <http://www.scia.org>.

# Appendix B–Acronyms

| | |
|---|---|
| ACL | Access Control List |
| CA | Certificate Authority |
| CC | Common Criteria for IT Security Evaluation (ISO/IEC 15408) |
| CCEVS | Common Criteria Evaluation and Validation Scheme |
| CD-ROM | Compact Disk—Read-Only Memory |
| CIO | Chief Information Officer |
| CMVP | Cryptographic Module Validation Program |
| COTS | Commercial Off-the-Shelf |
| CRL | Certification Revocation List |
| CVE | Common Vulnerabilities and Exposures |
| DBMS | Database Management System |
| DHCP | Dynamic Host Control Protocol |
| E-mail | Electronic Mail |
| Ext2FS | Second Extended File System |
| FAR | Federal Acquisition Regulation |
| FAT | File Allocation Table |
| FBCA | Federal Bridge Certification Authority |
| FFS | Fast File System |
| FIPS | Federal Information Processing Standard |
| FTP | File Transfer Protocol |
| GSA | General Services Administration |
| GUI | Graphical User Interface |
| HFS | Hierarchical File System |
| HTML | Hypertext Markup Language |
| HTTP | Hypertext Transfer Protocol |
| I&A | Identification and Authentication |
| ID | Identification |
| IDS | Intrusion Detection System |
| IP | Internet Protocol |
| IPSec | Internet Protocol Security |
| ISO | International Organization for Standardization |
| ISP | Internet Service Provider |
| IT | Information Technology |
| LAN | Local Area Network |
| LCC | Life-Cycle Cost |
| LDAP | Lightweight Directory Access Protocol |
| NAT | Network Address Translation |
| NIAP | National Information Assurance Partnership |
| NIST | National Institute of Standards and Technology |
| NSA | National Security Agency |
| NTFS | New Technology File System |
| OMB | Office of Management and Budget |
| OS | Operating System |
| OSI | Open Systems Interconnect |
| PC | Personal Computer |
| PCMCIA | Personal Computer Memory Card International Association |
| PDA | Personal Digital Assistant |

| | |
|---|---|
| PIN | Personal Identification Number |
| PKI | Public Key Infrastructure |
| PKIX | Public Key Infrastructure for X.509 Certificates |
| PP | Protection Profile |
| PROM | Programmable Read Only Memory |
| RA | Registration Authority |
| RADIUS | Remote Authentication Dial-in User Service |
| RBAC | Role-Based Access Control |
| RDBMS | Regional Database Management System |
| ROM | Read-Only Memory |
| SMTP | Simple Mail Transfer Protocol |
| SNMP | Simple Network Management Protocol |
| SSL | Secure Socket Layer |
| TACACS+ | Terminal Access Controller Access Control System + |
| TCP | Transfer Control Protocol |
| TLS | Transport Layer Security |
| UDP | User Datagram Protocol |
| UFS | Unix File System |
| WAN | Wide Area Network |
| WORM | Write-Once Read-Many |

# Appendix C–Frequently Asked Questions

**1. Why was this guide written?**

This guide seeks to help organizations make informed decisions when selecting computer security products. The categories of products listed here include operational controls such as intrusion detection and technical controls such as firewalls. This guide should be used with other NIST publications to develop a comprehensive approach to the management of an organization's computer security requirements. The guide first defines broad security product categories and then specifies product types within those categories. This guide explains and provides a list of characteristics and pertinent questions an organization should ask in the selection process.

**2. For whom is the guide intended?**

This guide is written to help an organization during the various stages of the computer security product life cycle. It can be used as a tool by—

- IT Security Officers in gathering the necessary information for the IT risk assessment and building the business case for the procurement of IT security products
- Chief Information Officers (CIO) and Chief Technology Officers (CTO) in establishing product procurement policy and ensuring that security has been appropriately considered in the selection process
- IT directors, program managers, and system owners in understanding the types of available security products, what they should consider when making a selection decision, and what factors they should use for evaluating a security product.

**3. Who has a role in product selection?**

Product selection involves numerous people throughout an organization. Each person involved in the process, whether on an individual or group level, should understand the importance of security in the organization's information infrastructure and the security impacts that their decisions will have. The personnel listed below are a sample guide. Depending on the organization's needs, one may include all of the personnel listed below or a combination of particular positions relevant to IT security needs.

- IT Security Program Manager
- Chief Information Officer
- IT Investment Board (or equivalent)
- Program Manager (owner of data) / Procurement Initiator
- Acquisition Team
- Contracting Officer
- Contracting Officer's Technical Representative
- IT System Security Officer

**4. What specific security products should an organization select?**

This guide does not discuss how an organization should develop its overall computer security program or the optimal set of products that should be implemented, nor are the product categories listed in this guide exhaustive as the commercial marketplace for IT security products is constantly changing. Also, the specific products that are right for each organization will vary based on mission, specific IT infrastructure, security objectives, costs, performance requirements, schedule constraints, operational constraints, and so forth.

**5. How should an organization go about selecting IT security products?**

A security program, whether at the organization or at the system level, should include an appropriate mixture of security controls: management, operational, and technical. The number and type of appropriate security controls and their corresponding IT security products may vary throughout a particular system's development and procurement life cycle. The relative maturity of an organization's security architecture may influence the types of appropriate security controls. The blend of security controls is tied to the mission of the organization and the role of the system within the organization as it supports that mission.

Risk management is the process used to identify an effective mix of management, operational, and technical security controls to mitigate risk to a level acceptable to the responsible senior official. Once the necessary controls are identified, IT security products can then be identified to provide for these controls. In addition, it is important to perform a cost-benefit analysis when selecting security products[1]. As part of the cost-benefit analysis, a life-cycle cost (LCC) estimate for the status quo and each alternative identified should be developed. In addition to LCC estimates, benefits associated with each alternative should be identified and, to the extent practicable, quantified in terms of dollar savings or cost avoidance.

Once all options are weighed in the cost-benefit analysis, the security product selection is made, and implementation of the product can follow.

**6. How can an organization gain assurance in the operation of the security features of commercial-off-the-shelf (COTS) products?**

Independent, third-party testing and evaluation of IT products can give consumers greater confidence that the security features in those products work as advertised by the vendor. Testing and evaluation also provides a way to demonstrate product compliance with organization security requirements and public security standards. Additionally, whether or not evaluated, the vendor's expression of security capability in the form of a Common Criteria Security Target (ST) enhances understanding of product claims by providing a standard format that includes rationale for correctness and completeness. NIST Special Publication 800-23 provides guidance on security assurance and the use of tested/evaluated products, and should be consulted by organizations selecting security products for their IT systems and networks.

- Two prominent security testing and evaluation programs are now in place to assess the security features and assurances of commercial off-the-shelf (COTS) products: (1) National Information

[1] There may be cases where the cost of a product is relatively low or the benefit is somewhat obvious, i.e. a virus scan product. In these situations, the rigor of a cost-benefit analysis may be reduced.

Assurance Partnership[2] (NIAP) Common Criteria (CC) Evaluation and Validation Scheme (CCEVS) and (2) NIST Cryptographic Module Validation Program[3] (CMVP). In the case of cryptographic modules, when agencies have determined the need to protect information via cryptographic means they may only select CMVP validated cryptographic modules. See http://csrc.nist.gov/cryptval/ for a validation list for cryptographic standards.

**7. What are the organizational considerations when selecting an IT security product?**

The organizational considerations required to support a product purchase are provided in the list of following questions. An organization may or may not have a need to consider all questions. In some cases, a high cost product acquisition may require a more extensive evaluation of organizational considerations.

- Is the anticipated user community identified? How many and what type of users does the organization anticipate will use the security product?
- Is the relationship between this security product and the organization's mission performance understood and documented?
- Has the sensitivity of the data the organization is trying to protect been determined?
- Are the organization security requirements supported by security plans, policies and procedures?
- Have security requirements been identified and compared against product specifications?
- Has appropriate procurement language been used for the specific product under selection?
- Have operational issues, such as daily operation, maintenance, contingency planning, awareness, and training, and documentation been considered?
- Have policies been developed for the procurement and use of evaluated products as appropriate? When selecting products, organizations need to consider the threat environment, the security functions needed to cost-effectively mitigate the risks to an acceptable level. Organizations should give consideration to procurement and deployment of IT security products that meet their requirements and have been evaluated and tested by independent accredited laboratories against appropriate security specifications and requirements. Examples of these specifications include protection profiles based on ISO/IEC 15408, the *Common Criteria for IT Security Evaluation*.
- Is communication required across a domain boundary (implies the need for a boundary controller; e.g., sub-system of firewall, intrusion detection system, and/or routers)?
- Are the system components (hardware or software) required for this product identified?
- Is the security product consistent with physical security and other policy requirements?
- Has the impact on the enterprise operational environment where this product will operate been considered?
- Has the impact of emerging technologies on the product been considered?
- Is the product necessary to mitigate risk?

[2] See http://niap.nist.gov
[3] See http://csrc.nist.gov

- Are the system components (hardware or software) required for this product identified?
- Have security reviews been made for support/plug-in components middleware?

**8. What are the product considerations?**

The following questions apply to the product and should be considered when forming a decision and selecting a product:

- Have total life-cycle support, ease-of-use, scalability, and interoperability requirements been determined? The total life cycle covers "cradle to grave" and hence includes security product disposal requirements.
- Have test requirements, for acceptance and integration testing, and configuration management been developed? If the product has been evaluated under the NIAP-CCEVS, validation test reports can be examined to avoid duplication of tests already performed as part of the independent evaluation process.
- Have known product vulnerabilities been addressed by reviewing the relevant vulnerabilities for a product? Known vulnerabilities for some products can be found using the NIST ICAT Vulnerability Search Engine (http://icat.nist.gov).4
- Have all relevant patches been tested and implemented?
- Have existing CC protection profiles (PP) been reviewed (for example, http://niap.nist.gov/cc-scheme/PPRegistry.html and http://www.commoncriteria.org/protection_profiles/pp.html), to identify PPs that express security requirements applicable to the organization's needs in the anticipated threat environment? If existing protection profiles are not adequate, organizations should consider the usefulness of similar protection profiles as a starting point for examining products that might satisfy requirements applicable to the new environment.
- Lists of validated products (for example, http://niap.nist.gov/cc-scheme/ValidatedProducts.html) should be reviewed. Products independently tested and validated under NIAP-CCEVS (or mutually recognized) provide some level of security assurance that the security functions of the product work as specified. In general, third party testing and evaluation can provide a significantly greater basis for customer confidence than is available from unevaluated products. Note, however, that purchasing an evaluated product simply because it is evaluated and without due consideration of applicable functional and assurance requirements and vendor reliability, may be neither useful nor cost effective. Organizations should consider their overall requirements and select the best products accordingly. The FIPS 140-1/FIPS 140-2 (CMVP) program's Validated Products lists (see http://csrc.nist.gov/cryptval) should be reviewed as the use of validated products is mandatory and binding on federal agencies where they have determined information must be protected via cryptographic means. This applies to all IT products irrespective of whether the product is a security product or whether the cryptographic module is embedded within another product (e.g. a database).
- Has the vendor's policy or stance on re-validation of products when new releases of the product are issued been considered?
- Have product specifications been reviewed with respect to existing and planned organizational programs, policies, procedures, and standards? Examples include an organization's

[4] ICAT is a search engine for an industry standard set of known vulnerabilities (http://cve.mitre.org) containing links to vulnerability and patch information.

- Web policy
- Public key infrastructure (PKI) program and policy
- Smart card program
- Network interconnection and approval policy.

- Does the product have any security critical dependencies on other products? For example, an operating system (OS) or cryptographic module?
- Does interfacing the new product with the existing infrastructure introduce new vulnerabilities?
- What is the frequency of product failures and adequacy of corrective actions?

**9. What are the vendor considerations?**

The following questions apply to the vendor and should be considered when forming a decision and selecting a product:

- Will the selection of a particular product limit the future choices of other computer security or operational modifications and improvements? (Note: The change and pace of technology may make it difficult to estimate the impact to an organization's future security architecture.)
- Does the vendor have experience in producing high quality IT security products?
- What is the vendor's "track-record" in responding to security flaws in its products?
- How does the vendor handle software and hardware maintenance, end user support, and maintenance agreements?
- What is the long-term viability of the vendor?
- Has the vendor developed a security configuration guide?
- Does the vendor have an associated security guide for the product? Does the vendor use or make reference to NIST, consortia, or other consensus-based checklists, security configurations/settings or benchmarks.

**10. Which IT security product categories are discussed in this document?**

The document discusses the following product categories of security products representative of common technological elements helpful in securing infrastructure:

- Identification and authentication
- Access control
- Intrusion detection
- Firewall
- Public key infrastructure
- Malicious code protection

- Vulnerability scanners
- Forensics
- Media sanitizing